LibraryVPN

A New Tool to Protect Patron Privacy

Chuck McAndrew

Due to increased public awareness of online surveillance, a rise in massive data breaches, and spikes in identity theft, there is a high demand for privacy enhancing services. VPN (Virtual Private Network) services are a proven way to protect online security and privacy. VPN's effectiveness and ease of use have led to a boom in VPN service providers globally.

VPNs protect privacy and security by offering an encrypted tunnel from the user's device to the VPN provider. VPNs ensure that no one who is on the same network as the user can learn anything about their traffic except that they are connecting to a VPN. This prevents surveillance of data from any source, including commercial snooping such as your ISP trying to monetize your browsing habits by selling your data, malicious snooping such as a fake wifi hotspot in an airport hoping to steal your data, or government-level surveillance that can target political activists and reporters in repressive countries.

Some people might ask why we need a VPN as HTTPS becomes more ubiquitous and provides end to end encryption for your web traffic. HTTPS will encrypt the content that goes over the network, but metadata such as the site you are connecting to, how long you are there, and where you go next are all unprotected. Additionally, some very important network protocols, such as DNS, are unencrypted and anyone can see them. A VPN eliminates all of those issues.

However, there are two major problems with current VPN offerings.

First, all reliable VPN solutions require a paid subscription. This puts them out of reach of economically vulnerable populations who often have no access to the internet in their homes. In order to access online services, they may rely on public internet connections such as those provided by restaurants, coffee shops, and libraries. Using publicly accessible networks without the security benefits of a VPN puts people's security and privacy at great risk. This risk could be eliminated by providing free access to a high-quality VPN service.

The second problem is that using a VPN requires people to place their trust in whatever VPN company they use. Some (especially free solutions) have proven not to be worthy of that trust by containing malware or leaking and even outright selling customer data. Companies that abuse customer data are taking advantage of vulnerable populations who are unable to afford more expensive solutions or who do not have the knowledge to protect themselves. Together, these two problems create a situation where having security and privacy is only available to those who can afford it and have the knowledge to protect themselves. Libraries are ideally positioned to help with this situation. Libraries work to provide privacy and security to people every day. This can mean teaching classes, making privacy resources available, and even advocating for privacy-friendly laws.

Chuck McAndrew (chuck.mcandrew@leblibrary.com) is Information Technology Librarian, Lebanon (NH) Public Libraries.

https://doi.org/10.6017/ital.v39i2.12391

Libraries are also located in almost every community in the United States and enjoy a high level of trust from the public. Librarians can be thought of as being a physical VPN. People who come into libraries know that what they read and information that they seek out will be protected by the library. In fact, libraries have helped to get laws protecting the library records of patrons in all 50 states of the USA. People know that when a library offers a service to their community it isn't because they want to sell their information or show them advertisements. With libraries, our patrons are not the product.

Libraries also already provide many online services to all members of their community, regardless of financial circumstances. Examples include access to online databases, language learning software, and online access to periodicals such as the *New York Times* or *Consumer Reports*. Many of these services would cost too much for individual patrons to access individually. By pooling their resources, communities are able to make more services available to all of their citizens.

To help address the above issues, the Lebanon Public Libraries, in partnership with the Westchester (New York) Library System, the LEAP Encryption Access Project (https://leap.se/), and TJ Lamanna (Emerging Technology Librarian from Cherry Hill Public Library and Library Freedom Institute Graduate) started the LibraryVPN project. This project will allow libraries to offer a VPN to their patrons. Patrons will be able to download the LibraryVPN application on a device of their choosing and connect to their library's VPN server from wherever they are.

LibraryVPN was first conceived a number of years ago, but the real start of the project was when it received an IMLS National Leadership Grant (LG-36-19-0071-19) in 2019. This grant was to develop integrations between LEAP's existing VPN solution and integrated library systems using SIP2 which will allow library patrons to sign in to LibraryVPN using their library card. This grant also included development of a Windows client (there was already a Mac and Linux client) and alpha testing at the Lebanon Public Libraries and Westchester Library System. We are currently working on moving into the testing phase of the software, and planning phase two of this project.

Phase two of LibraryVPN will involve expanding our testing to up to 12 libraries and conducting end-user testing with patrons and library staff. We have submitted an application for IMLS funding for phase two and are actively looking for libraries that are excited about protecting patron privacy and would like to help us beta test this software. If you work for a library that would be interested in participating, you can reach us via email at libraryvpn@riseup.net or @libraryvpn on twitter.

If you would like to help out with this project in another way, we would love to have more help. Please reach out.

We currently are thinking about three deployment models for libraries in phase two.

First would be an on-premises deployment. This would be for larger library systems with their own servers and IT staff. LibraryVPN is free and open source software and can be deployed by anyone. Since it uses SIP2 to connect to your ILS, it should work with any ILS that supports the SIP2 protocol. This deployment model has the advantage of not requiring any hosting fees but does require the library system to have staff that can deploy and manage public facing services. Drawbacks to this approach would include higher bandwidth use and dealing with abuse complaints. Phase 2 testing should give us better data about how much of an issue this will be, but our experience hosting a Tor exit node at the Lebanon Public Libraries suggest that it won’t be too bad to deal with.

Our second deployment model would be cloud hosting. If a library has IT staff who can deploy services to the cloud, they could host their own LibraryVPN service without needing their own hardware. However, when deploying to the cloud, there will be ongoing costs for running the servers and bandwidth used. Figuring out how much bandwidth an average user will consume is part of the data we are hoping to get from our phase 2 testing so we can offer guidelines to libraries who choose to deploy their own LibraryVPN service.

Finally, we are looking at a hosted version of LibraryVPN. We anticipate that smaller systems that do not have dedicated servers or IT staff will be interested in this option. In this case, there would be ongoing hosting and support costs, but managing the service would not be any more complicated than subscribing to any other service the library hosts for their patrons.

LibraryVPN is a new project that is pushing library services outside of the library to where the library is. We want to make sure that all of our patrons are protected, not just those with the financial ability and technical know-how to get their own VPN service. As librarians, we understand that privacy and intellectual freedom are joined, and we want to maximize both. As the American Library Association’s Code of Ethics says, “We protect each library user's right to privacy and confidentiality.”