Find out how students are circumventing the web filter at school

and what you can do to prevent it

Linewize
by Family Zone

HOW ARE STUDENTS CIRCUMVENTING THE FILTER?

It's no secret that K-12 students aren't exactly thrilled with the idea of being blocked from browsing certain content online. And with students today only growing up knowing life with the internet and technology surrounding them, they have become more and more technologically smart. But filters have gotten smarter as well.

Find out how students are circumventing the web filter at school—and what you can do to prevent it.

Circumvention

VPNs were legitimately designed to mask traffic from hackers and align with the privacy movements in the US today—and they're readily available. The reality is, anyone can download a VPN on Google Play to get around most security systems at schools. Students today are far more technologically advanced than they ever have been, and at younger ages. This means that determined children know how to access VPNs, proxy servers and other anonymizer sites that are used to mask traffic and bypass the filter. Let's take a deeper dive into what each of these circumvention methods are about.

VPNs

Virtual private networks (VPNs) are a common way for students to attempt to circumvent the web filter that may be in place at school or at home.

Example:

A student downloads a VPN onto a USB or on their phone when connecting to a school network. All the network can see is that this student is making an encrypted VPN connection and sending data via that connection. The specific VPN connection would have to be blocked in order to prevent the student from continuing that action. The problem is that schools enter into a game of “whack-a-mole” as a multitude of VPNs pop up every day.

Top 10 VPNs Attempted to be Used by Linewize Customers

1. Ultrasurf
2. Psiphon
3. Tor
4. BetterNet
5. OperaVPN
6. Hotspot Shield
7. Tunnelbear VPN
8. Zenmate VPN
9. Chrome Browser VPN
10. DashVPN

circumvention TECHNIQUES

Proxy Websites

In order to avoid installing anything on their devices, students are also looking to standard proxies to attempt to get around the filter. A proxy website is one that may look like https://www.hidenseek.org/ for example, but when you browse there, it allows you to browse the internet freely without every changing the site in the URL bar. It is essentially a browser within a browser that doesn't reveal where the user is actually going. If they are looking to quickly access a blocked website, often times a proxy is the route to go.

Top 5 Proxy Websites Attempted to be Used by Linewize Customers

1. cIP-C
2. New IP Now
3. Hide.me
4. H1de
5. Proxy Site

With so many VPNs popping up regularly, many IT admins find themselves chasing down VPN URLs and direct IP addresses so they can block them, but it's a game of cat and mouse. It's almost impossible if you have a DNS-based web filter. With a layer 7 web filter, the signatures break quite often and need to be updated regularly.

If a bank employee tried to use a VPN to bypass security systems so that they could view pornography at work, they'd be fired—maybe even arrested. When it happens in a school environment by a student, it's IT's fault—and you have to give them the device again the very next day. So how can you prevent students from leveraging VPNs and other circumvention tactics to get around the filter?

Chasing down VPN URLS

WHAT YOU CAN DO TO PREVENT IT

Linewize has looked at the problem a bit differently—we look at how VPNs fundamentally function so that behaviors are easily recognizable as attempting to circumvent the filter. VPNs use brute force—if one URL is blocked, it tries another. If that URL is blocked, it tries direct IP access. If that is blocked, it spoofs SNI or DNS records to indicate it is a legitimate service. It tries the same techniques on different UDP or TCP ports as well. If one of those attempts is successful, it will have a large, encrypted stream of traffic to a single IP address or URL which we can identify as abnormal compared to legitimate browsing traffic.

THE LINEWIZE PLATFORM

Using two very specific techniques to identify VPNS—machine learning to identify the differences between known VPN traffic and legitimate user traffic—and auto-quarantining techniques to snip bits of traffic for further investigation and verification, our technology is able to block VPNs as they pop up. Because Linewize School Manager is a true hybrid deployment option, it has visibility to look at each of the scenarios listed above. In addition, our product dissects and updates signatures for the main VPNs such as Betternet, Psiphon, Ultrasurf, TOR, Hotspot Shield, and many more.VPNs are always going to be tough to block, but School Manager is the best in the market at doing so. Stop playing whack-a-mole with your VPNs and leave this hard work up to us at Linewize.

Linewize Ecosystem

Linewize School Manager

- ✓ AI to capture evasive applications
- ✓ One-to-one on or offsite
- ✓ Identify indicators of cyberbullying, self-harm, & violence

Linewize Classwize

- ✓ Integrated screen visibility with filter
- ✓ Granular control of student tabs
- ✓ Promote responsible digital citizenship

Family Zone Community

- ✓ Educate community on cyber safety
- ✓ Digital cyber safety course
- ✓ Engage parent community

Find out more with a demo.

www.linewize.com ● SAFEWEB (844-723-3932)

Linewize