



Cloud vs. Appliance Web Filtering

Choosing the right web filter for
large district deployments

For years, an on-site filtering appliance was a common solution for schools wanting to keep students and student devices safe on-campus. However, when devices began going home, the limitation of an appliance's reach became more evident. In particular, the scalability and effectiveness became growing concerns for the IT Administrators from large school districts responsible for providing students with a safe web browsing experience outside of the classroom.

Cloud-based solutions are not subject to the same limitations as appliances by nature of their being infinitely scalable and effective no matter where devices go.

Benefits of a cloud-based solution include:

Fault Tolerance

No single point of failure or reliance on services that are on-premises

High Performance

Responds immediately to increased demand

Ease of Authentication

User Injection and SSO options for zero-touch authentication

Turn-key SSL Decryption

Set up out of the box and crowdsourced from other schools

Let's take a closer look at how each option stacks up in these four areas.

Fault Tolerance

Appliances

If an on-site appliance is slowed by increased traffic or, worst-case scenario, goes down completely, web filtering is affected or completely lost. A single point of failure means that if one thing goes wrong, it all goes wrong.

Cloud-based solutions

Securly is hosted and distributed throughout multiple AWS Clusters, all with built-in redundancy. If one server goes down, another one automatically takes its place and service remains uninterrupted.

Performance

Appliances

On-site appliances require PAC files, a JavaScript function that looks at a requested URL or host and decides whether to proxy the URL or let it through. Proxying is done when a site is blocked or if there's cause to perform deep packet inspection (ex: keywords within the query). Challenges with PAC files include:

- Schools must manually update static Allow/Deny lists
- Many applications and sites break when proxied
- Reliant on on-prem authentication source (e.g. Active Directory or LDAP)
- Proxying back to on-prem filters requires open firewall ports which compromise network security
- Proxying traffic back to the school for offsite filtering turns your school into an ISP for 1:1 devices, meaning if your network is down, so is your offsite filtering
- To handle the increase in bandwidth, many schools are required to have exponential pipes to the internet with redundancy and failover

Cloud-based solutions

Securly developed SmartPAC, which provides uniformity across the install base by removing the need to update a static file. By leveraging our cloud-based infrastructure, development included user-injection and verbose logging, allowing 1:1 schools to define it only proxies by need and without sacrificing dynamic reporting. SmartPAC allows the

user who learns on that device to never have to authenticate with Securly ever again, both on-site and off. Besides being 100% cloud-based, benefits of Securly Filter include:

- Any browser, any device
- Rich reporting
- User, URL, search keywords, and MITM SSL decryption
- Provides per-student or per-OU policies
- Zero-touch Google/Azure/AD authentication
- Portable & easily maintained code
- Minimal local footprint (<10K bytes)

Turn-key SSL Decryption

Appliances

Not built specific to the needs of K-12, but rather a clientele made up of medium to large corporate entities. Maintenance of the hardware, as well as updating of databases, are manual operations required of individual administrators.

Cloud-based solutions

Built specifically for K-12, Securly's cloud-based filtering automatically decrypts what is important to schools, (e.g. which keywords a user searches, what videos a child watches). Securly manages and maintains these databases so customers never have to. Over 10 million daily active users and tens of thousands of schools contribute to a hive mind to ensure all children receive equal safety measures.

Ease of Authentication

Appliances

If 1:1 devices and users are participating in learning from multiple locations, being tied down to routing authentication back to the school's Active Directory is simply not practical. Authentication is impossible if the appliance becomes unavailable due to a loss of power or broadband connection.

Cloud-based solutions

Securly natively supports Google and Azure, plus authenticates users no matter where they are located—at home or at school. Securly can also support and leverage local active directory as a single-sign-on solution, thereby streamlining, if not completely removing, the need for students to use their username or password to get online. For example, a first-grader with an iPad is already authenticated the moment their device turns on, associating their device and activity for reporting.

Summary

When looking at cloud-based vs. appliance-based filtering, major differences including fault-tolerance, high performance, turn-key SSL decryption, and ease of authentication, showcase the ever-growing divide between the two solutions of their long-term viability.

When your school district has a need for scalable and reliable web filtering, the limitations of appliances are painfully clear and the benefits of cloud filtering are impossible to ignore.

To learn more the benefits of a cloud web filter designed specifically for K-12 schools, visit www.securly.com/filter



✉ sales@securly.com

☎ 1-855-SECURLY

🌐 www.securly.com