ContentKeeper

White Paper

Why SSL Decryption Is Critical for Today's School Web Filters — and Five Keys to an Effective Solution

Over the last few years, there has been a seismic shift in how Google, Facebook, and other leading websites handle Internet security—and this shift has enormous implications for school web filtering.

The rise of Secure Sockets Layer (SSL) encryption has made it harder to monitor and filter students' Internet use effectively. Makers of Internet filtering products have responded to this challenge by building SSL decryption capabilities into their software, but the quality of these solutions varies widely.

In this white paper, you'll learn what SSL decryption is and why it matters. You'll also learn about the challenges involved in SSL decryption and how these have led to a big gap in effectiveness among solutions. Finally, you'll get a five-point framework for evaluating Internet filtering solutions to make sure the product you choose can handle SSL decryption successfully.

Without SSL decryption, Internet filtering and monitoring tools can only see the top-level domain of a requested website. They can't see the full path of the request: They can't see keyword search terms or what kind of content is returned.

SSL Decryption — and Why It Matters

SSL is the standard security technology for establishing an encrypted link between a web server and a browser. It ensures that the data passed between the web server and browser remains private, so hackers can't intercept this information as it is being transmitted. Websites that begin with the URL string "https" instead of "http" are using SSL encryption.

As recently as a few years ago, SSL encryption was used primarily by banks and online vendors to provide secure e-commerce transactions. But in 2012, Facebook began using SSL encryption for all of its web pages; the following year, Google began using the technology for all of its web searches. Today, nearly all social media sites and Internet search engines — including YouTube — use this security protocol.

Without SSL decryption, Internet filtering and monitoring tools can only see the top-level domain of a requested website. They can't see the full path of the request: They can't see the keyword search terms typed in search engines, or what kind of content it returned. Decrypting the communication between the server and web browser, however, allows web filters to see the full URL string of the requested website as well as any content returned, enabling the filters to be far more effective.

Here's how this works: The filtering solution would decrypt the session request, inspect the full URL string, and compare it to the software's filtering rules. If the requested web page is permitted, the filter then would re-encrypt this request before passing it along to the appropriate server.

Here are four reasons why this ability is critical for schools:

More precise control.

If your Internet filtering system doesn't have SSL decryption, then you can't have granular control over the specific web pages or features within YouTube, Facebook, and other social media sites.

You can only block or allow access to the top-level domain. That means you would have to let students access all of YouTube, for example — or else block all YouTube videos altogether.

Neither of these scenarios is desirable for educators. Along with some inappropriate content, YouTube also contains a wealth of useful educational content — and teachers want to be able to filter out inappropriate videos while having access to appropriate ones in class. SSL decryption allows for this more precise level of control.

In fact, ContentKeeper has developed a new feature that makes this process easier for instructors, called Real-Time Video Whitelisting. If a YouTube video comes from a trusted source, such as a learning management system or a specified domain, ContentKeeper whitelists it in real time and allows the video to play — without a teacher having to contact the IT department to request access first.

Without SSL decryption, students easily can use any one of the millions of proxy bypass servers on the Internet, allowing them to slip past most filtering systems undetected. The encrypted session provides no information for the filtering system to detect the activity and block or control it. ContentKeeper decryption effectively provides visibility, blocking, and control of SSL-based proxy bypass sites.

More detailed reporting.

If your Internet filtering solution can only see the top-level domain for SSL-encrypted web traffic, then that's the only information you would see in an Internet use log. If a student requested a specific Facebook page, for instance, all that would appear in your report is www.facebook.com. But with SSL decryption, you can see the exact web page that is accessed or denied.

There are many ways this could be useful, such as for investigations. In one recent case, the FBI contacted a Florida school to request its Internet use logs, because the agency suspected one of the school's teachers of pedophilia. But the logs only showed that he had accessed www.instagram.com 300 times from a school computer; investigators couldn't determine whether he was accessing the Instagram profiles of specific students.

The widespread use of SSL encryption has made it appealing for hackers to disguise their attacks within SSL-protected sessions. Without a deeper inspection of SSL-encrypted web traffic to make sure it's legitimate, you could be exposing your schools to greater risks.

Keyword search analysis.

Because Google and other search engines now use SSL encryption, there is no way of knowing what keywords your students are searching for unless your filtering solution can decrypt these requests.

But if your Internet filter supports SSL decryption, then you can see which keywords your students are Googling, because these keywords appear in the full URL string of the search query. And ContentKeeper has developed a feature that uses this visibility to add another layer of protection for students and staff.

Called Real-Time Behavioral Profiling, this feature analyzes keyword searches in real time, along with the sites that are accessed, and notifies a designated administrator if someone searches for a term that suggests a potential threat to himself or others. For example, if a student searches for the keyword phrase "how to kill myself," the system would trigger an automatic alert, so an administrator could intervene immediately. Profiling can also be used to detect bullying, radicalization, or other potential dangerous behavior.

Greater protection from online threats.

The widespread use of SSL encryption has made it appealing for hackers to disguise their attacks within SSL-protected sessions. Without a deeper inspection of SSL-encrypted web traffic to make sure it's legitimate, you could be exposing your schools to greater risks.

SSL decryption allows for this deeper inspection and provides a higher level of security, helping to ensure that users aren't visiting spoofing or phishing sites and that downloads don't contain malicious content.

Not All SSL Decryption Is the Same

SSL decryption is critical for all of these reasons, but it also creates significant engineering challenges —and how an Internet filtering solution is designed has a big impact on its effectiveness.

Because the need to decrypt and re-encrypt web traffic adds more steps to the inspection process, SSL decryption typically slows Internet speeds down, often quite dramatically. If your Internet filter takes a proxy-based approach, you'll notice a huge difference in network performance when you apply SSL decryption — and this difference is multiplied as you add more users to the network.

A bridge-based filtering approach can work better, but only a few web filtering manufacturers utilize a bridge-based design — and they have only done so relatively recently.

That's not the case with ContentKeeper. The company has been using bridge filtering for the last 18 years — long enough to have perfected this approach. In fact, ContentKeeper's new TurboBridge technology runs on a revolutionary Ethernet bridge that supports filtering and decryption at multi-gigabit speeds, allowing organizations to migrate to 10 gigabit-per-second networks and beyond.

ContentKeeper's third-generation SSL Decode Engine provides fast, accurate, and selective decryption, so you can control which domains you want to decrypt and when.

What's more, ContentKeeper's third-generation SSL Decode Engine provides fast, accurate, and selective decryption, so you can control which domains you want to decrypt and when.

Indiana's DeKalb County Central United School District is using ContentKeeper to provide Internet filtering and security to its 3,800 students in six schools. Systems Administrator Matthew Dillinger said the district needed a solution that could decrypt SSL traffic, because officials wanted to be able to see which websites their students were searching for on Google. When Dillinger discovered that the system also provided very granular control over specific pages within social media sites, he was doubly impressed.

"We have not noticed any slowdown in our bandwidth," he said. "And the Web 2.0 controls are phenomenal. We can let students access certain parts of websites that are educational and filter out the parts that are not. I use them every chance I get."

What to Look for in a Filtering Solution

Given the importance of SSL decryption, and the fact that not all solutions are created equal, what should you look for when choosing an Internet monitoring and filtering solution for your schools? Here are five key criteria:

- **Can you take a very granular approach to blocking web pages within top-level domains, even those that are SSL-encrypted?** The solution must be able to decrypt SSL traffic so you can block certain pages or functions within Facebook, YouTube, and other social media sites, while allowing access to others if desired.

- **Can you see the full URL string in your Internet usage reports?** You should be able to see exactly which pages within SSL-encrypted websites your students or staff have accessed or tried to access, as well as which keywords they have searched for using Google or other Internet search engines.

- **Does the solution provide real-time behavior analysis of keyword searches, complete with automated alerts?** If someone is searching for information that can help them do harm to themselves or others, you don't want to have to wait until you inspect your Internet use logs (perhaps several days later) to know this. You want to be able to take immediate action.

- **Can you control when to turn off or apply SSL decryption based on certain factors?** Solutions must provide both selective as well as full decryption capabilities. They must allow you to bypass SSL decryption for certain types of websites while decrypting others, as there might be some website categories or domains you don't want to decrypt. Having the capability to do selective decryption lets you find the right balance between throughput speed and security.

- **Can the solution easily scale?** Before buying, test any solution you're evaluating at full scale with SSL decryption turned on to see how this affects your network speeds. You might be surprised at how widely this varies among products.

While SSL decryption can reduce network speeds — in some cases, quite dramatically — that's not a problem with ContentKeeper's TurboBridge technology and third-generation SSL Decode Engine.

The Bottom Line

Your Internet filtering solution must be able to decrypt SSL web traffic to protect students and staff from potentially harmful content, while giving them access to the tools and resources they need for success.

But beware: Many solutions are still very immature. They don't provide the necessary tools to deploy SSL decryption technology successfully. They often end up crippling your network and IT resources, and costing your organization dearly.

While SSL decryption can reduce network speeds — in some cases, quite dramatically — that's not a problem with ContentKeeper's TurboBridge technology and third-generation SSL Decode Engine. ContentKeeper's superior design can decode, inspect, filter, and log the full URL string for SSL-encrypted web traffic at multi-gigabit speeds — resulting in exceptional visibility and control over website requests with no noticeable network latency.

ContentKeeper's proven, in-depth solution provides educational institutions with all the tools they need to deploy, control, and manage their SSL traffic successfully.

Try it for yourself! Email **k12@contentkeeper.com** to set up a free demonstration.

ContentKeeper

ContentKeeper.com k12@ContentKeeper.com US: +1 888.808.6848 Intl: +61 2 6261 4950