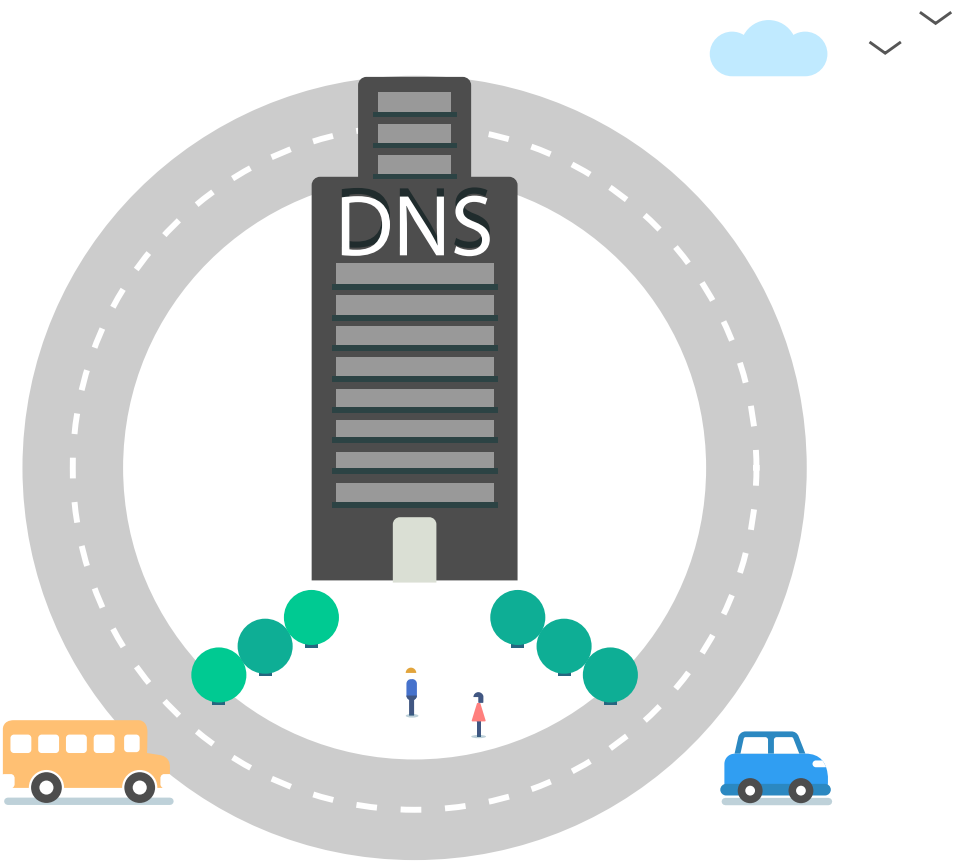
securly://

DNS to Anything - How Securly Works

APRIL 2018 | *by* Manasi Kulkarni



ABSTRACT

This paper discusses the architecture behind Securly's DNS-based filtering solution, currently making over 3 million US students safer. The steps for configuring a school network to use Securly's DNS-based filtering solution are laid out. Additionally, included statistics provide evidence of lives saved and bullying incidents mitigated as a result of these solutions.

CONTENT

INTRODUCTION

Each year, millions of students are handed school-owned devices in order to research topics for class or explore personal interests at home. Still, online dangers are only ever just a few mouse clicks away. Searching out adult content in a hormone-fueled fervor, cyberbullying a classmate over their race, using a parent's credit card to buy weapons, or conversing with strangers who may be online predators. As a result, schools are on the lookout for solutions that keep students both focused and safe. DNS-based solutions are easy to roll out and sweeping in their potential. Securly filters out inappropriate content, but also helps to prevent cyberbullying, self-harm, and even suicide in students. Keeping kids safe is a full-time job, but it doesn't have to be a difficult one.

DEFINITION OF TERMS

1. **DNS:** Domain Name Servers(DNS) are servers that contain a directory of domain names and convert them into IP addresses whenever a request is sent by a user. Securly maintains its own DNS servers used by its DNS filtering solution.

2. **Proxy server:** A proxy server works as an intermediary between the user's computer and the endpoint machine to fetch information from the endpoint website on behalf of the user. A proxy server can help control which websites students/users can and cannot access.

3. **Broker:** Broker is a web component that is central to the DNS solution and is used to identify the user, his policy, and category of the domain requested. Every request must necessarily pass through the broker for filtering to work correctly.

4. **Decryption:** Information/data on websites may be encrypted during transmission. The process of translating encrypted data into the understandable or original format is decryption. Securly does selective decryption of sites for filtering, activity logging, and sentiment analysis. (*Note- Securly does not decrypt sensitive information, or personal identifiable information(PII) such as credit card numbers, etc.*)

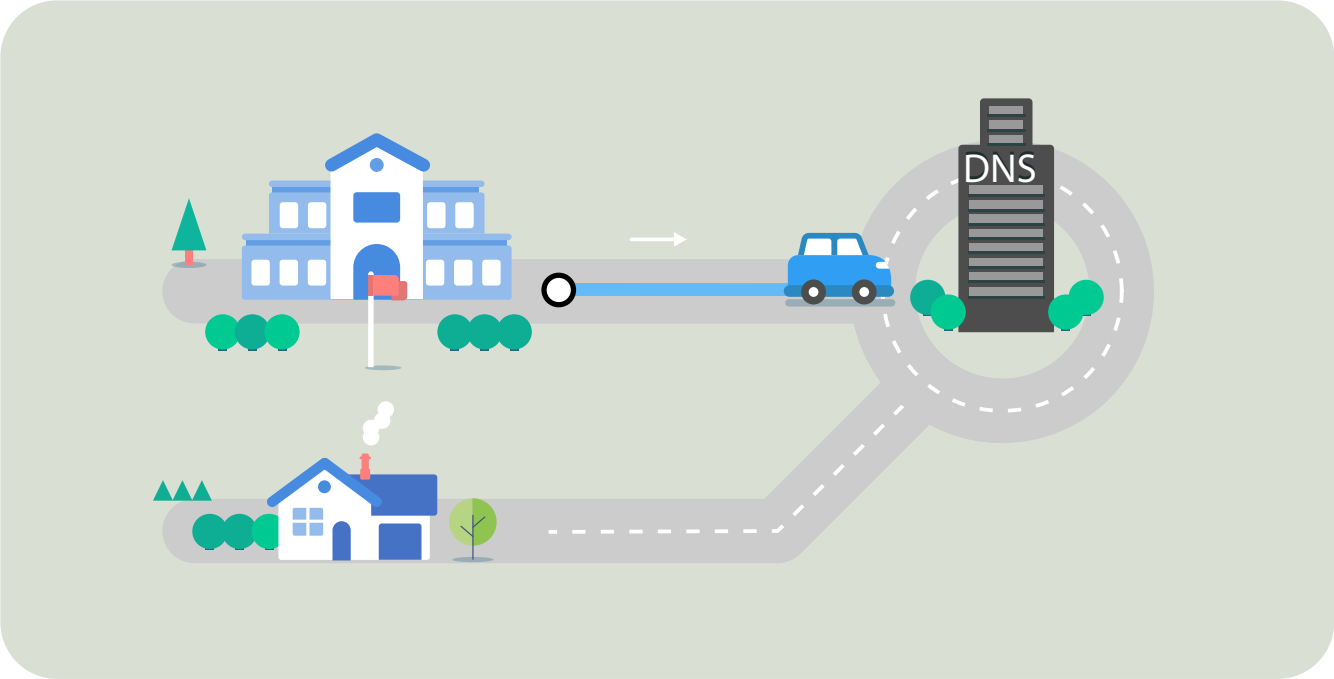
5. **Token:** A string of unique characters generated for a website once the user is logged in. The Securly server uses tokens to determine what filtering policy needs to be applied to the user.

6. **PageScan:** This is Securly's proprietary approach to auto-blacklisting new and potentially dangerous websites. It actively scans any new websites for inappropriate content and images, categorizes, and adds it to the Securly database such that any subsequent request to it is filtered appropriately.

UNDERSTANDING THE SECURLY DNS FILTERING ARCHITECTURE

Get, set, go...

When a student enters a website address (URL) into the browser, that request is sent to Securly's DNS, which replies with a Securly proxy address before sending it back to the student's machine.



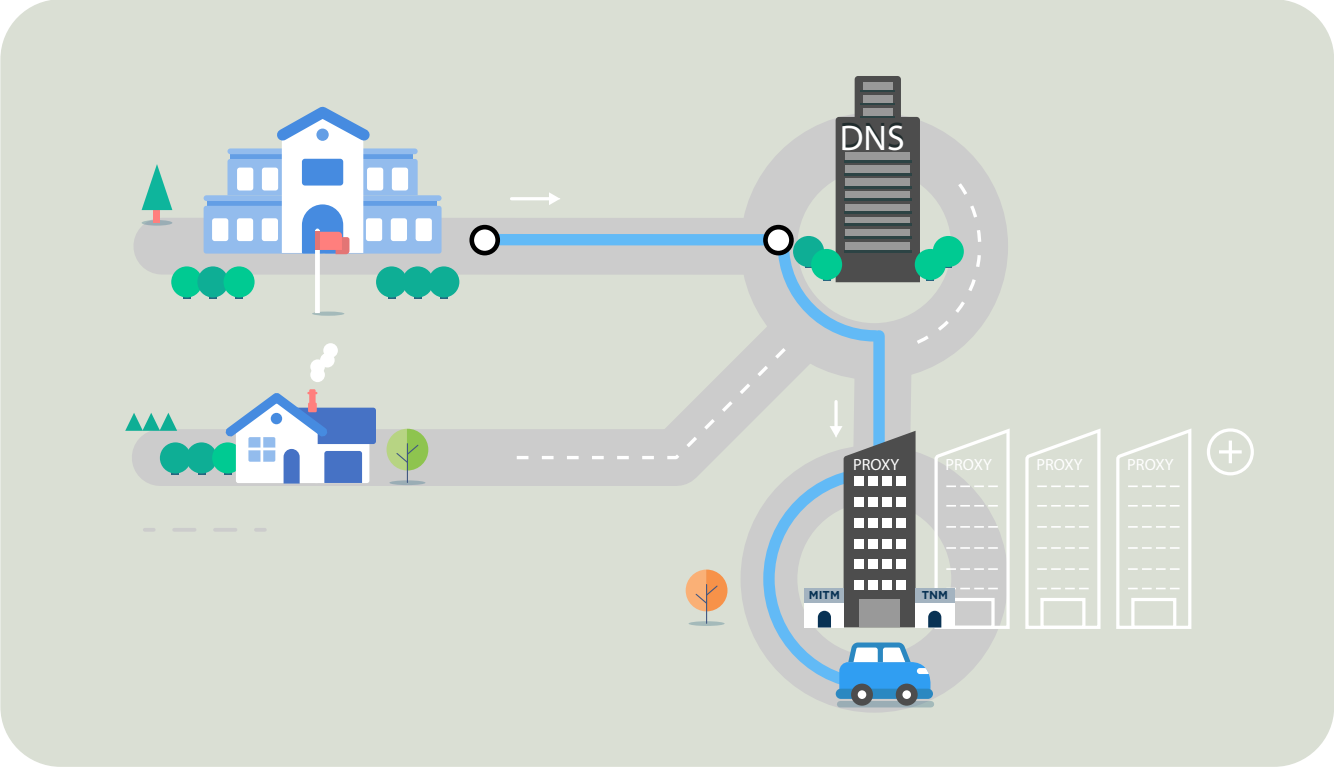
A visit to the proxy server

The traffic routes to the Securly proxy server. Securly maintains two types of proxy servers:

- MITM
- Non-MITM (TNM)

Depending on what type of website the student is trying to access, it will be sent to either of these two servers.

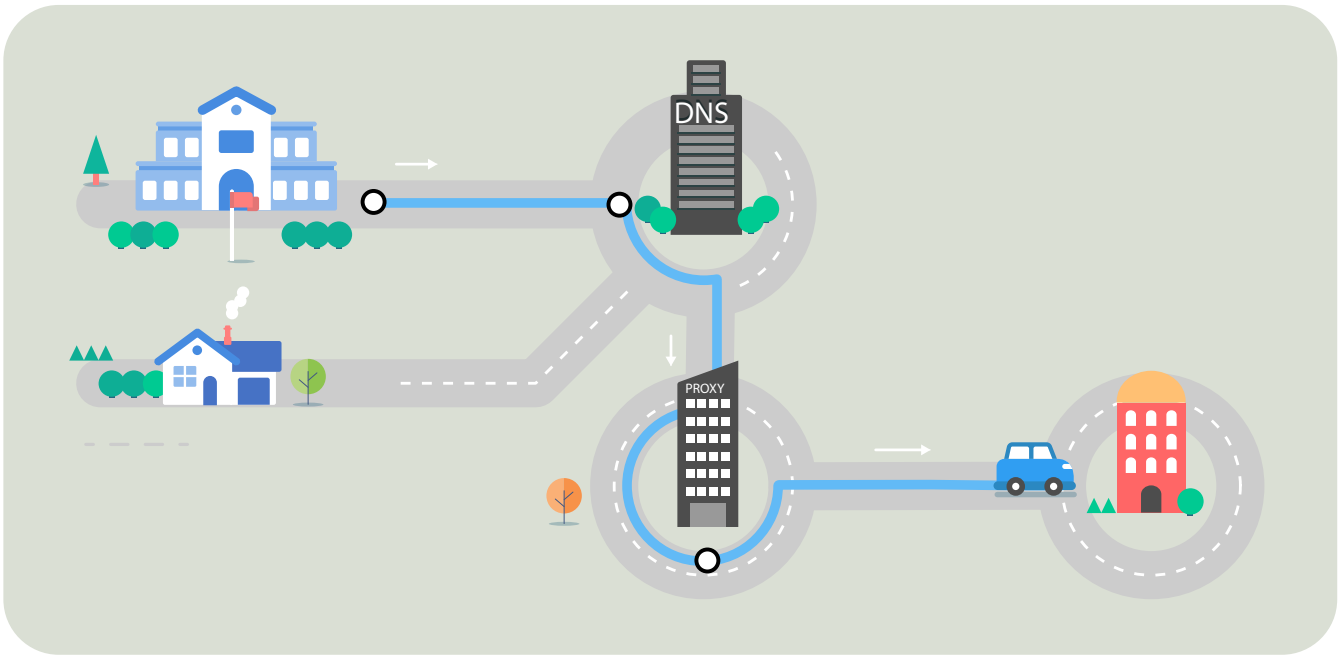
Being a 100% cloud-based service allows Securly to maintain an army of proxy servers that auto-scale depending upon the traffic load. Servers sleep and wake up as the traffic load fluctuates and ensure that users always get the same blazing fast DNS resolution no matter what traffic you throw at it.



Sites that need to be decrypted are sent to the MITM or Man-in-the-Middle server, so that Securly can act as the middleman for communication between students and websites. Social media sites often need to be decrypted to allow Securly's AI engines to monitor and flag self-harm, grief, bullying, and suicide-related posts. The sentiment analysis algorithm uses natural language processing to identify the sentiment behind posts. For example, "I have had enough, I cannot take this anymore," does not include any alarming keywords, but is still a clear indicator of grief in the student. This critical step in Securly's student safety initiative has already helped save lives.

Pitstop- User Authentication

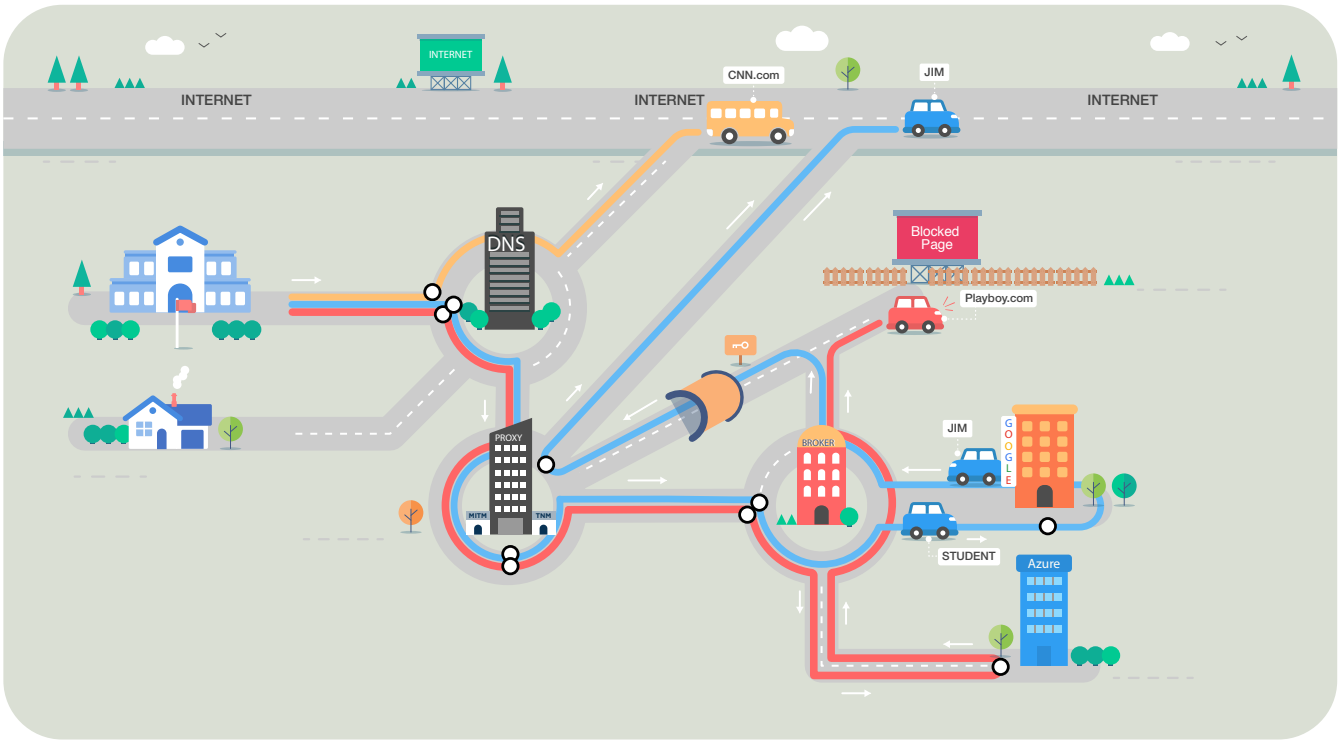
The proxy server then sends a request to the broker to help identify the user. At this stage, if the user is not signed in he/she is required to login and authenticate. Securly supports authentication with Google, Azure, and on-prem AD. The user would need to input his/her relevant login credentials at this stage and authenticate himself/herself as a valid user. The user would not be able to proceed further if authentication fails.



User information is usually stored in cookies, meaning users will not need to authenticate themselves again so long as he/she does not terminate the browsing session. If the user does terminate the session, then starts a fresh one on the same machine, they would be required to authenticate again.

Finish line

Once authenticated, the user's request is sent to the proxy server with the token information and the appropriate filtering policy applied. If the site the student is attempting to access is allowed as per school policy, he/she would continue to the actual website. If the site is blocked, student will receive a blocked page announcement. Irrespective of whether the student accesses the website or is shown a blocked page, all activity will be logged in the Securly database, and displayed to the school admin and parents within their Securly accounts. Any alarming activity will be flagged and sent to admins and parents via email.



This four step process happens real-time and does not interfere with the browsing experience of the user. Even at peak traffic hours, Securly's auto-scaling mechanism ensures that the filtering process remains fast and accurate. This process guarantees schools a comprehensive filtering experience where students are protected from harmful and age-inappropriate content at all times.

EXCEPTIONS

It should be noted that Securly has categorized over a million websites and counting in its database. This database is updated daily by Securly's proprietary PageScan technology that scans and categorizes new websites. Any site in this database will follow the four step filtering process. Any missing sites would stop at Step 1 and will be accessible to the user directly. However, such a site will be identified by PageScan and added to the Securly database within a few seconds for the next time any user attempts to access it.

Along with user based filtering, Securly also provides IP based filtering. This IP based filtering is used for the Guest Network Policy that allows schools to provide guests filtering access to their network, without requiring them to login.

HOW TO SET UP SECURLY DNS?

Setting up Securly DNS is a simple five minute process. Depending upon what type of environment you use at your school you would need to add the Securly DNS server information at your Firewall settings level, or Windows server settings level, or your router level. The Securly DNS details will be provided to you by the Securly sales engineer.

You would also need to install Securly SSL certificates to allow us to decrypt websites efficiently. You could do this at the browser level, device level or push out the certificates via your G Suite admin console. The Securly sales engineer will provide you the necessary SSL certificates during the onboarding process, or can be downloaded from **support.securly.com.**

SAVING LIVES WITH SECURLY DNS

Securly goes beyond basic filtering to include the detection of grief, bullying, and even suicidal tendencies in students. This is achieved using a sophisticated sentiment analysis algorithm that reads the actual sentiment behind posts, even when traditionally flagged keywords are not included. Securly constantly updates its database consisting of thousands of words, phrases, and sentences categorized to help the engine identify activities to be flagged.

In addition to its AI, Securly has a dedicated team of student safety analysts who investigate flagged activities to determine their severity, allowing parents and schools to intervene when necessary. Since the beginning of the 2018 school year, the 24 team has saved over 20 lives and managed to avert over five severe bullying incidents.

CONCLUSION

Saving lives is often attributed to a superhero carrying a busload of kids over a ravine or a firefighter leaping from a burning building with a baby in each arm. The reality is, saving lives can be far less dramatic and as simple as changing DNS settings. With Securly's DNS-based filtering solution, any school district's IT admin can become a life-saving hero in a matter of minutes.