Lightspeed Systems

SSL EXPLAINED

Lightspeed Systems

Table of Contents

Lightspeed Systems

Introduction

SSL is a challenge when it comes to school networks. From understanding what SSL is all the way to how Lightspeed Systems Web Filter can help you filter SSL traffic, this guide covers everything you need to know.

- What is SSL and why does it matter?
- The challenges of SSL and school networks
- Google, Youtube, and SSL
- Web Filtering and your SSL options

What is SSL?

You've probably heard the acronym "SSL," especially lately, in relation to Google. But you might not fully understand what it is, why it matters, and how Lightspeed Systems deals with the challenge.

So what is SSL?

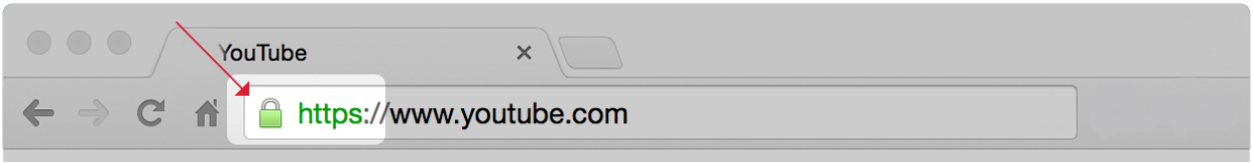


Figure 1

You've gone to a website and seen a little lock icon next to the Web address. This lock means that the data going to and from your computer is encrypted via SSL.

Most website's addresses start with *HTTP*; that means that the data transferring to and from your computer and the website's server is in plain text.

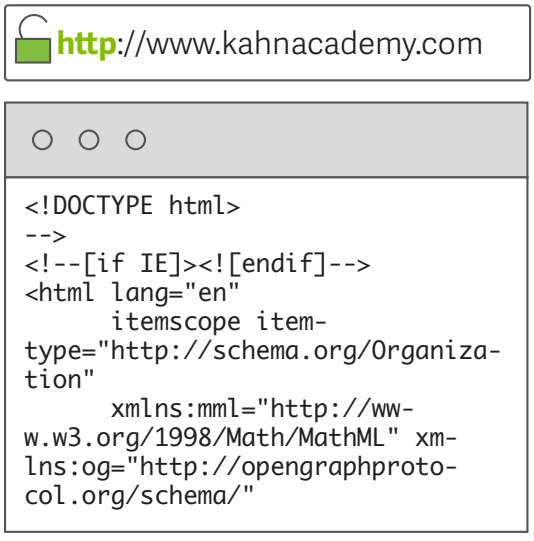


Figure 2 http (unencrypted data can be easily read)

But when you pay for something with your credit card on Amazon, or you log into your bank account, you don't want that information transferred in plain text. The Internet is a wide, open place, and anyone who has the skills can see that information. If that information is transferred in plain text, it's relatively easy to steal.

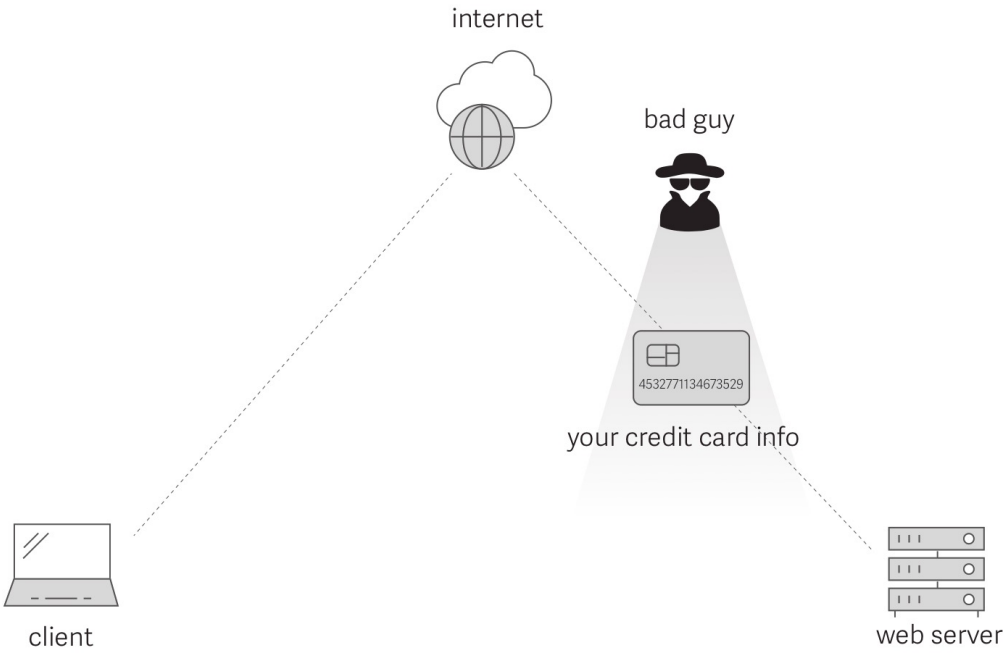


Figure 3

There is another way to start Web addresses, and that is HTTPS (the "s" stands for secure). With HTTPS transmissions, the information passing from your computer to the website's server is encrypted, so that the data cannot be read by any third parties.

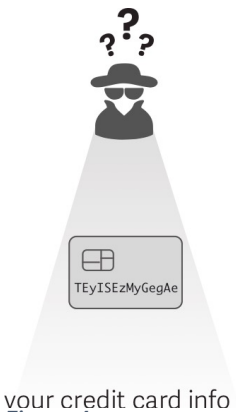
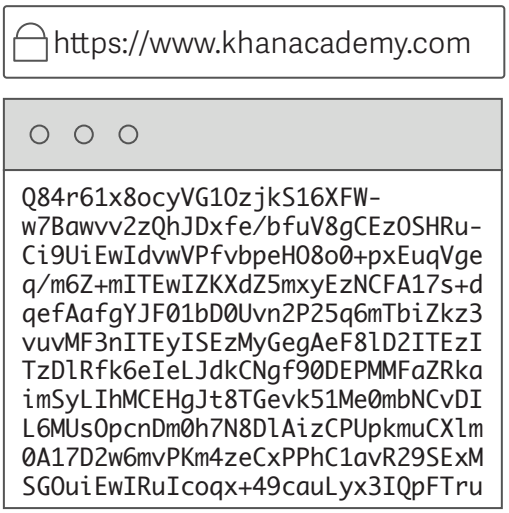


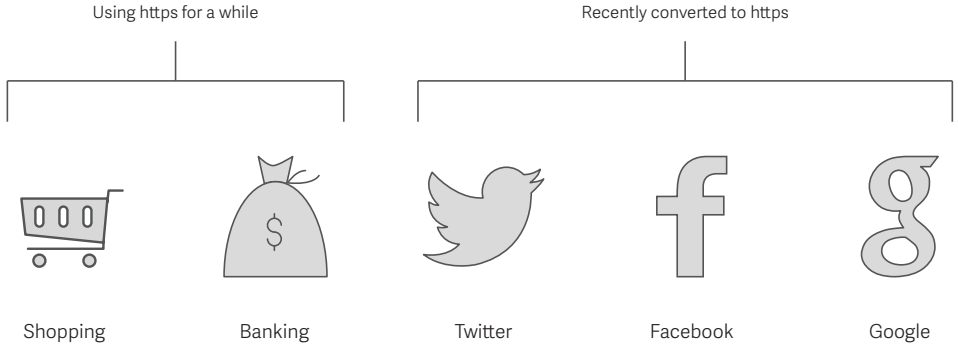
Figure 4



Historically, HTTPS was used for sites that stored critical information (e.g., banks), but over time, more and more websites (such as Google, Facebook and Twitter) have made the switch because of privacy concerns.

Figure 5 https (encrypted data cannot be read without the key)

Figure 6



Google switching all its services (including Google Apps for Education, Google Docs, Google Play, YouTube, etc.) to HTTPS is problematic for schools. If all the information going between student devices and Google is encrypted, Web filtering becomes a challenge. How do schools balance privacy with their responsibility to keep kids safe? Fortunately, Lightspeed Systems has you covered

How does SSL work?

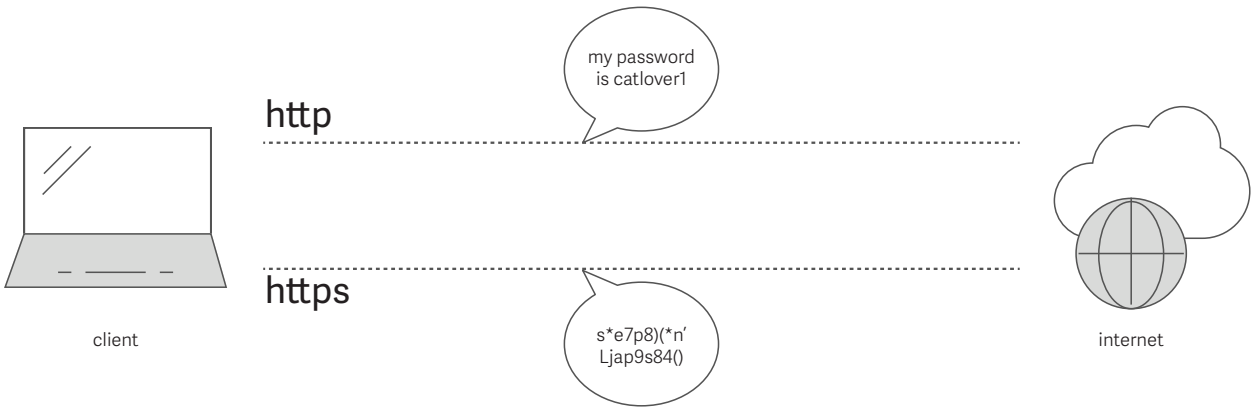


Figure 7

SSL, which stands for Secure Sockets Layer, is a security protocol that creates an encrypted connection between a computer and a Web server.

Basically, it's a series of steps that the browser and the server agree upon that set up the encrypted connection.

Figure 8

The way that they do this is by exchanging an SSL certificate. The certificate is basically a digital document that:

- authenticates the identity of the website
- provides the digital signature of the certificate authority who issued the certificate
- provides the website server's public encryption key

Figure 9

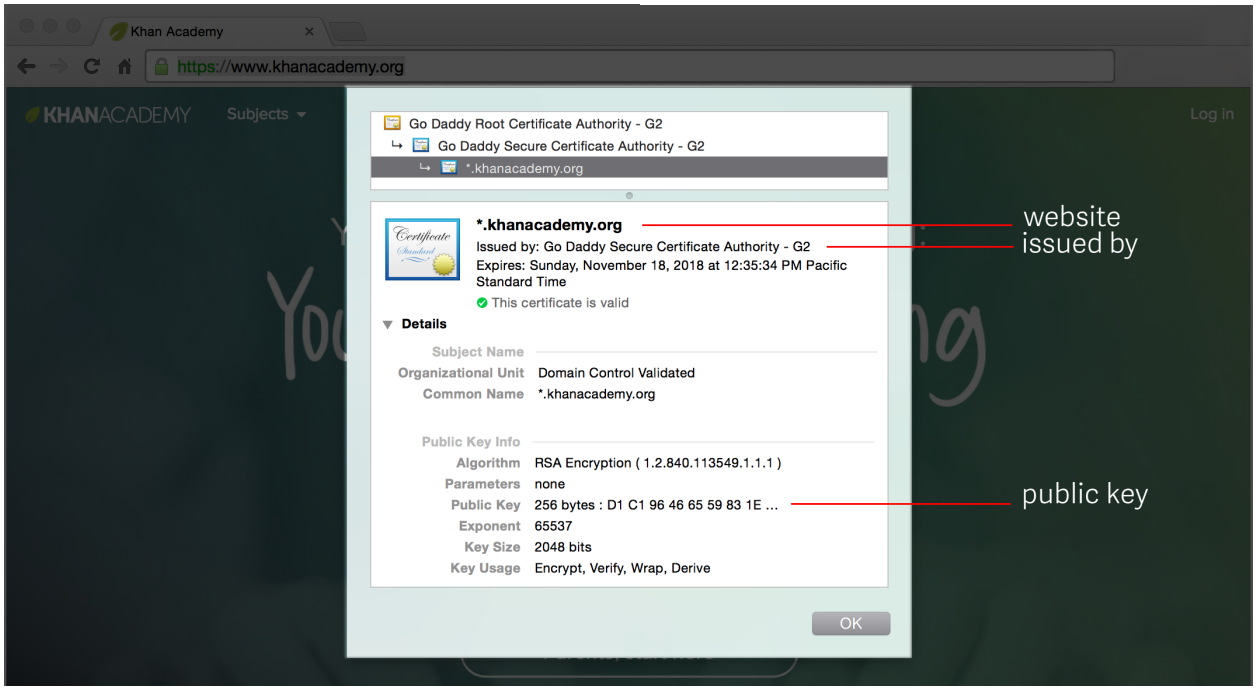


Figure 10 Example SSL Certificate in a browser

Website: khanacademy.org

Your computer compares the name of the website that you typed into the Web address bar with the name of the website on the certificate. If they don't match, then some other person or entity may be posing as Khan Academy.

Issued by: Go Daddy

It is possible for anyone to create an SSL certificate. For that reason, it's important that you trust the entity who issued the certificate. Modern Web browsers are installed with trusted root certificates, so usually your computer trusts the certificate authority. If the Web browser does not trust the issuer, then it will warn you to proceed at your own risk.

Public Key

As you can tell, the public key is a very complicated set of numbers and letters. This public key is the key that your browser will use to create the encryption. The public key is used to encrypt the data, and the client (your computer) creates a secret key that can decrypt the data sent by the website's server.

The back-and-forth between the client and the Web server is referred to as a handshake. Here's how the handshake works:

1. You type into your Web address bar the name of a website (e.g., www.google.com)
2. Your computer sends a message to Google's server.
3. Google's server replies to your computer and sends its SSL certificate to the client.
4. Your Web browser verifies the SSL certificate and creates a secret key (password) that is encrypted with the public key so no third party can read it.
5. The server uses the secret key to encrypt the data and sends it to the Web browser.
6. The Web browser decrypts the message and displays it as HTML in your Web browser.

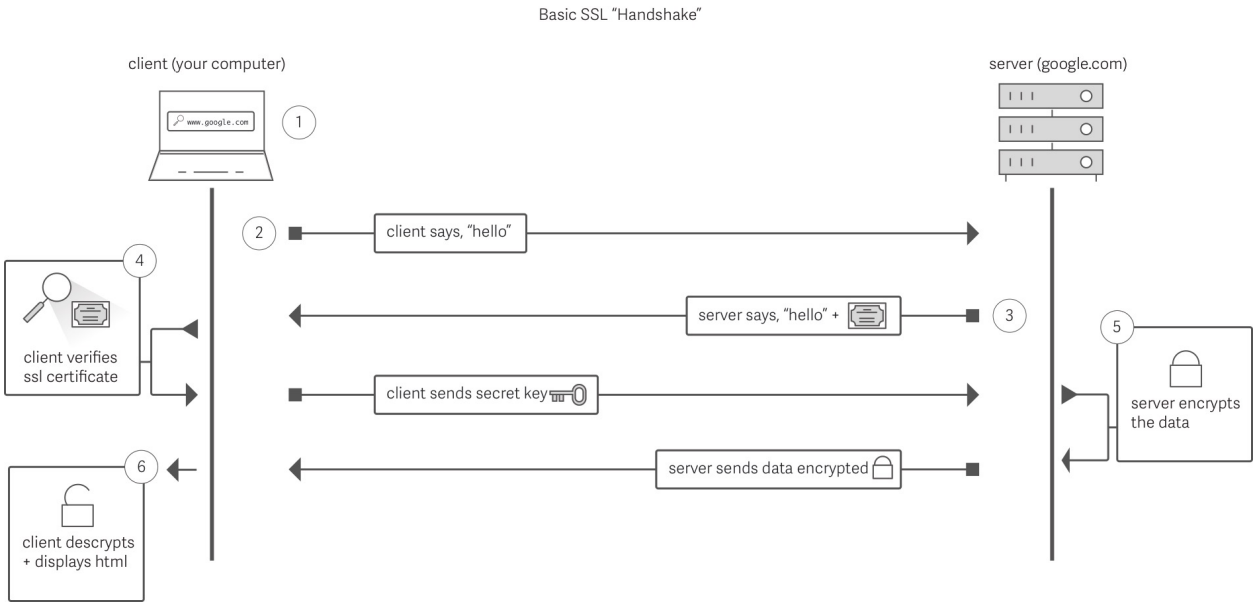


Figure 11

And that is how SSL works.

Google & SSL

As previously mentioned, the SSL certificate sent by the server includes the identity of the website. For instance, that means that if you navigate to www.khanacademy.com, its SSL certificate will name the site *khanacademy.org.

However, there is a type of SSL certificate that Google uses called a wildcard SSL certificate. A wildcard SSL certificate is used for an unlimited number of subdomains. For Google, its subdomains include:

- Google Drive
- Google Docs
- Google Play
- YouTube
- and many more

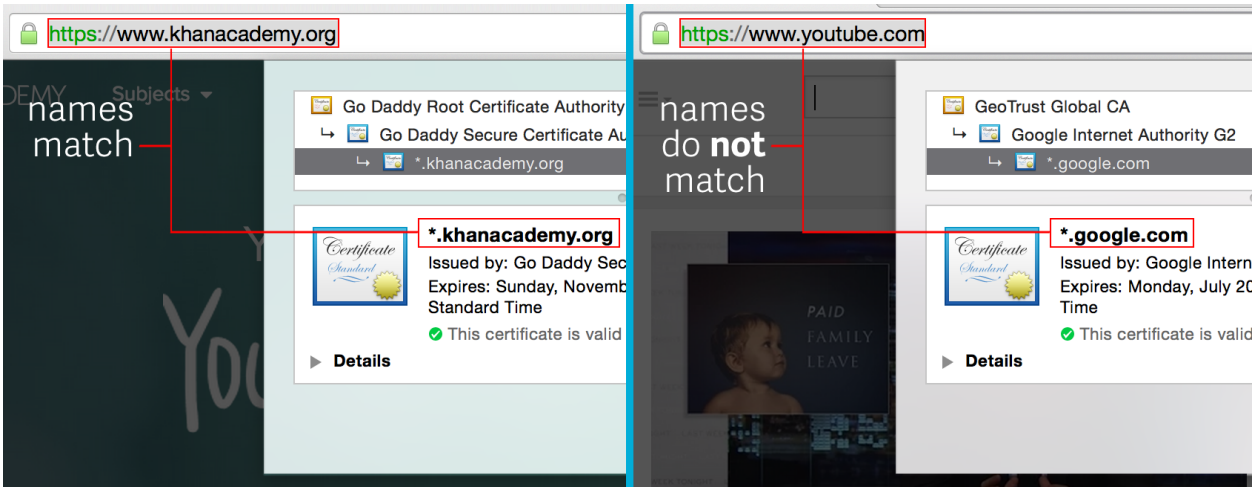


Figure 12 You cannot distinguish between any of the google subdomains based on the SSL certificate

In addition to the SSL wildcard certificate problem is the general problem of URL detail with SSL connections. There is also no way to know what the client is browsing within the site based on the SSL certificate information alone.

For schools, it is important to know full URL details for Google and YouTube. The full URL allows you to know what was searched for on Google and what was viewed on YouTube. With the SSL certificate information, you only know the domain, not the full URL.

Figure 13

SSL/TLS

SSL (Secure Sockets Layer) is a blanket term that typically refers to SSL or TLS (Transport Layer Security).

TLS was developed as the successor to SSL. It is a better, more modern version of SSL (and it is still being updated). When the client and server initiate the handshake, they decide whether to use SSL or TLS. Most modern Web browsers support TLS, but some older ones don't.

In Web filtering, TLS is superior to SSL. When using TLS, there is a critical piece of information that is available for the Web filter to decode. That is the SNI, or Server Name Indication. The SNI allows your Web filter to get the actual domain you are going to rather than the host that is listed on the SSL certificate.

Let's use YouTube as an example: The SSL certificate would read *google.com, whereas the SNI would indicate youtube.com.

Web Filtering SSL

A typical network (without a Web filter) can be represented by the below image.

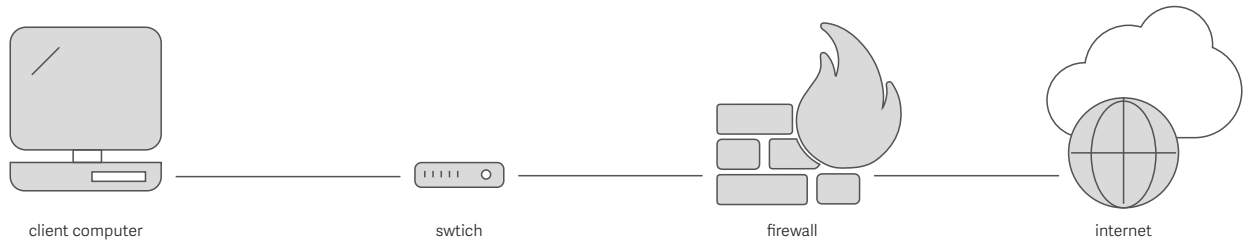


Figure 14

The client computer sends out a request. The SWITCH sends that request to the appropriate place. The FIREWALL allows the traffic out to the INTERNET while stopping bad requests from coming in but allowing the good requests.

In this type of network, individual users (clients) have complete freedom to go anywhere on the Internet without being filtered.

A Web filter is important in environments in which you need to protect the network (and its users) from inappropriate materials while allowing appropriate use.

A Web filter sits between the user (client) and the Internet. The filter goes through requests and makes decisions on whether to block or allow based on the policies that you set, and then it creates reports of the activity and the sites that have been accessed.

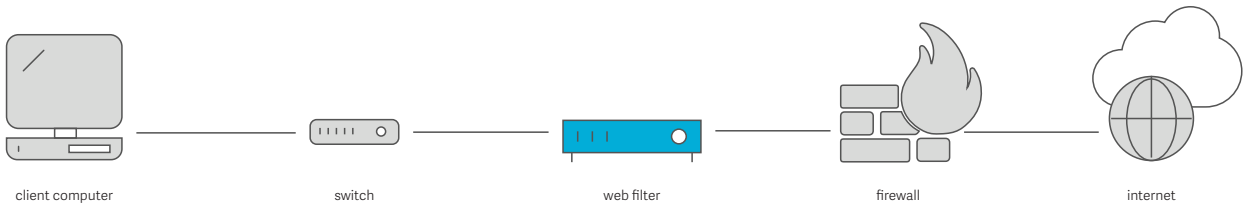


Figure 15

When it comes to schools, Internet access and Web filtering, there is a lot to consider. You need to protect student and teacher privacy, but you also must follow acceptable guidelines and your school's AUP. Ultimately, you must also protect students from inappropriate content while giving them access to rich educational content. SSL makes balancing these needs difficult.

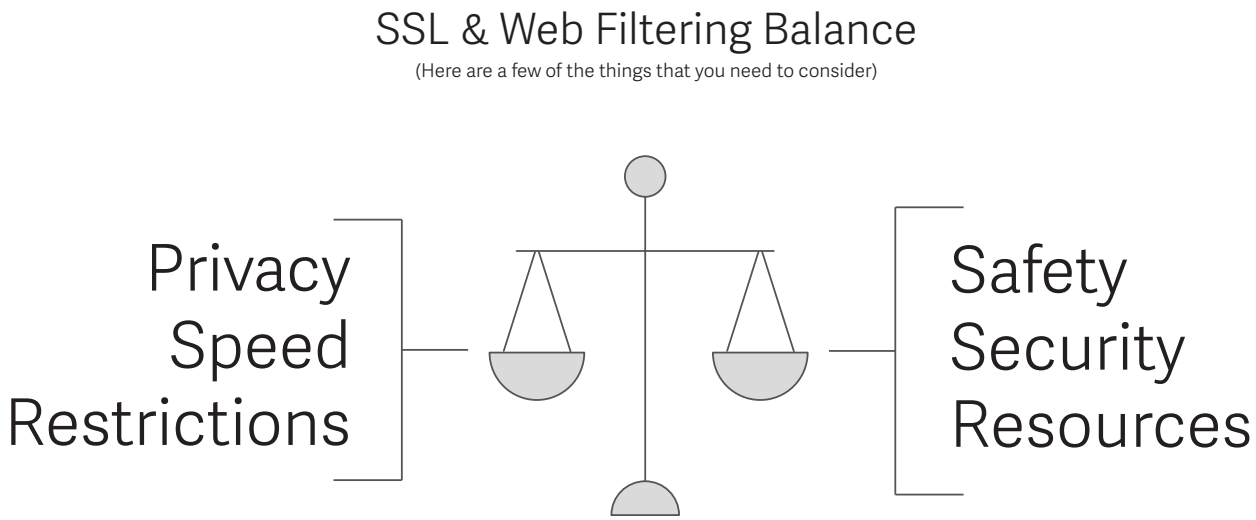


Figure 16

When you are trying to set up a Web filter so that you can manage what users have access to (and what they do not have access to), you need to know where they are going in order to say "yes" or "no".

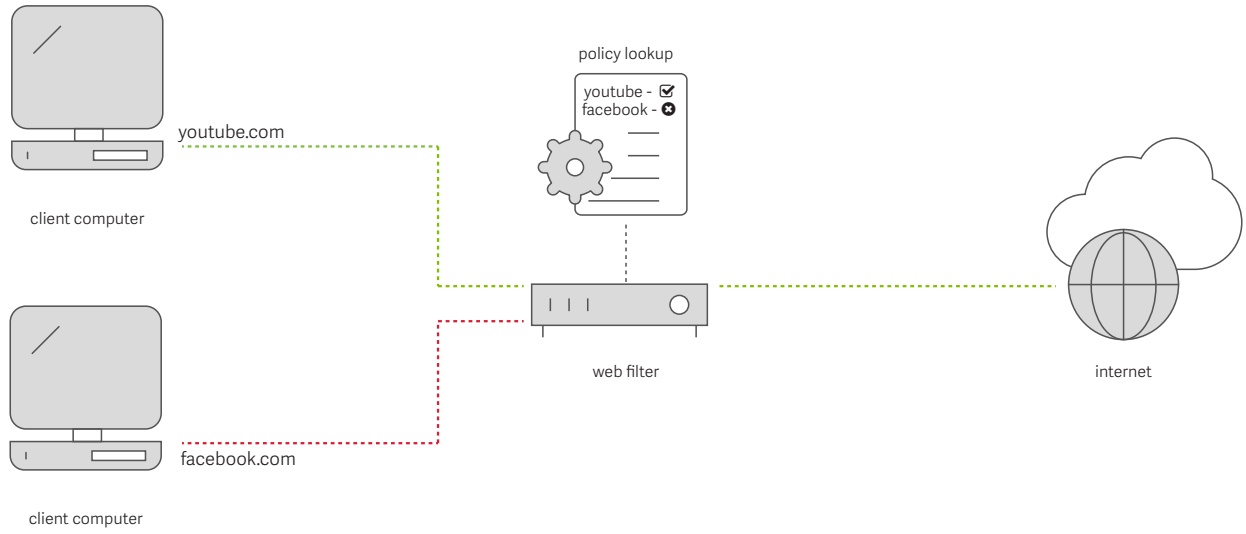


Figure 17 web filter set up to block web sites based on policies

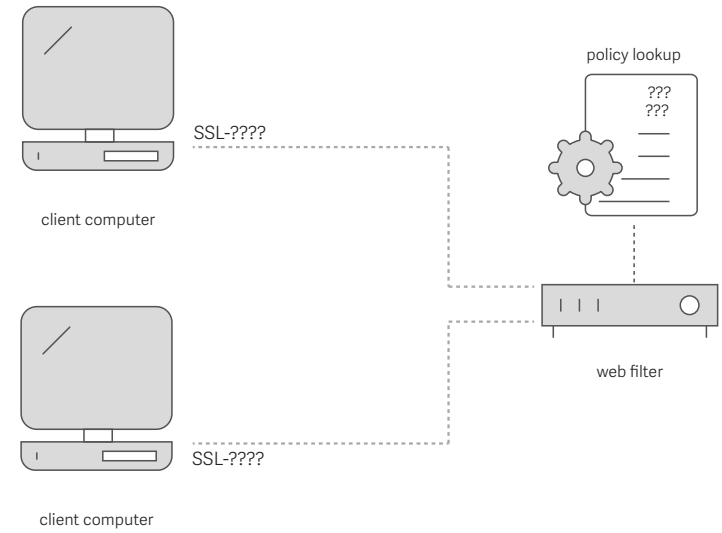


Figure 18

SSL blocks this information from being seen by default, so without a properly configured Web filter, you will not be able to block/allow websites based on policies — because you won't know where your traffic is going.

The problems mentioned above are universal problems for organizations, enterprise and education included. As such, there are a few options for filtering Web traffic and handling SSL specifically.

1. Block SSL traffic

This is the most restrictive, but safest, option. What this effectively means is that you will not be able to go to Google, YouTube, Khan Academy, and many more educational websites.

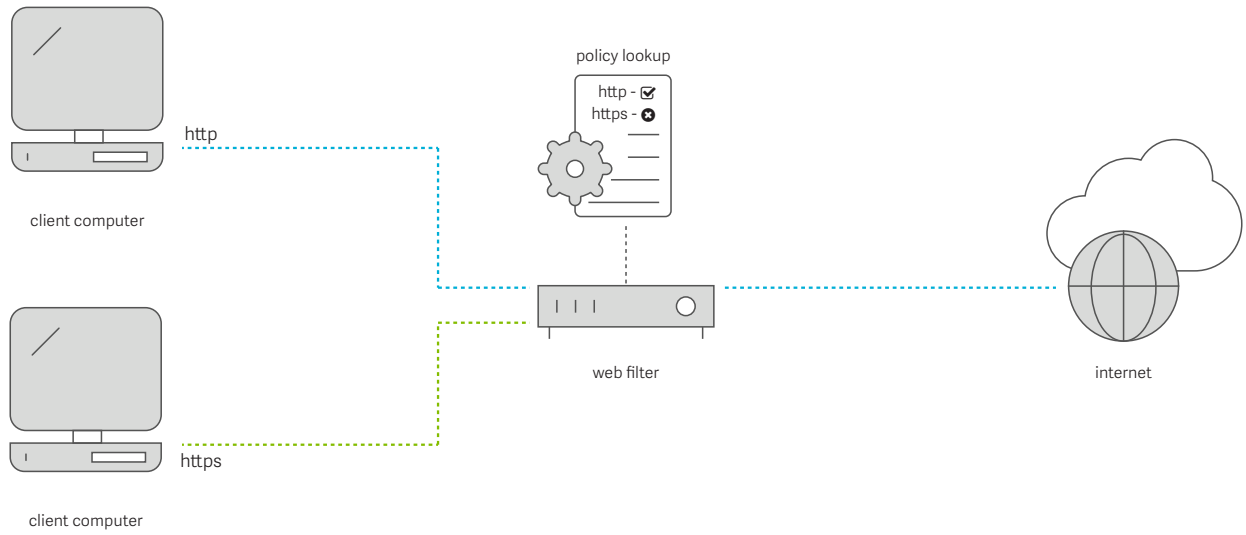


Figure 19

Considering how many websites are HTTPS (SSL) websites, this is incredibly restrictive and will likely result in some very upset teachers and students.

2. Decode SSL traffic

This option inspects SSL certificates and SNIs, if they are being used, and controls traffic through block/allow lists. This is a less severe option than completely blocking SSL because you can selectively allow or disallow

sites. (For instance, you can allow khanacademy.com and disallow facebook.com.)

1. Client initiates the handshake with the requested website. The web filter lets the traffic pass through to the web server.
2. Web Server continues handshake and sends SSL certificate.
3. The web filter inspects the certificate (and SNI when available) and checks the site against the policies. If it is allowed then it passes the traffic through to the client.

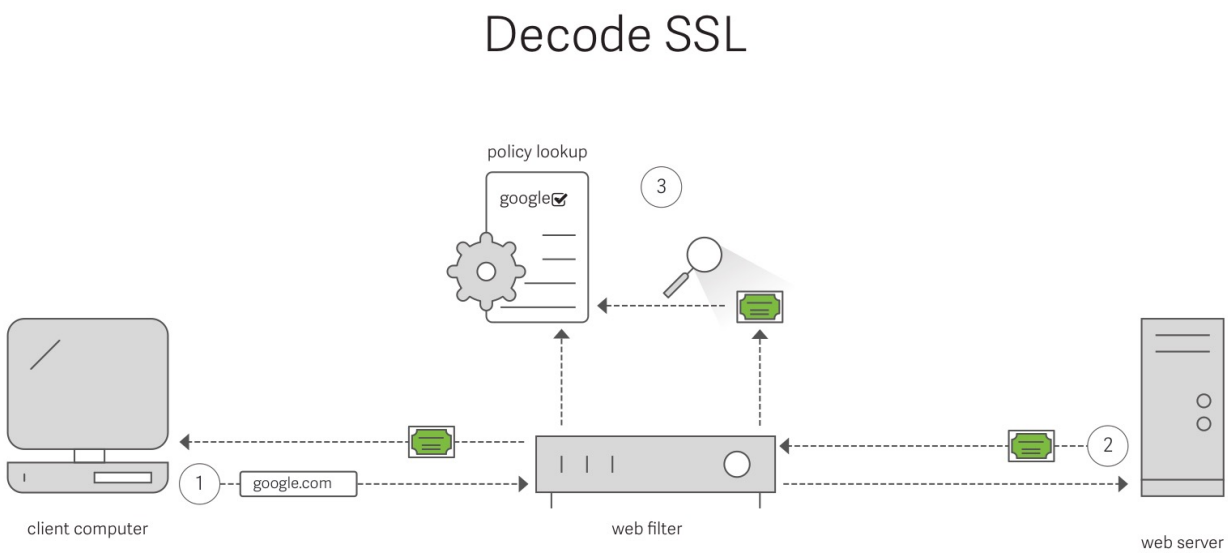


Figure 20

When you decode SSL, you can get domain information, such as youtube.com or google.com. You can't see full URL details, so you won't see what the user searched or what videos he watched.

3. Decrypt SSL traffic

Remember when we mentioned earlier that no one can decrypt the SSL encrypted connection? That isn't entirely true. You can secure special permission to decrypt SSL traffic.

If you use this method, encrypted SSL traffic is decrypted and read as plain text, just like traditional HTTP connections. This method offers the least privacy, but the greatest security. This method is typically referred to as "trusted man in the middle."

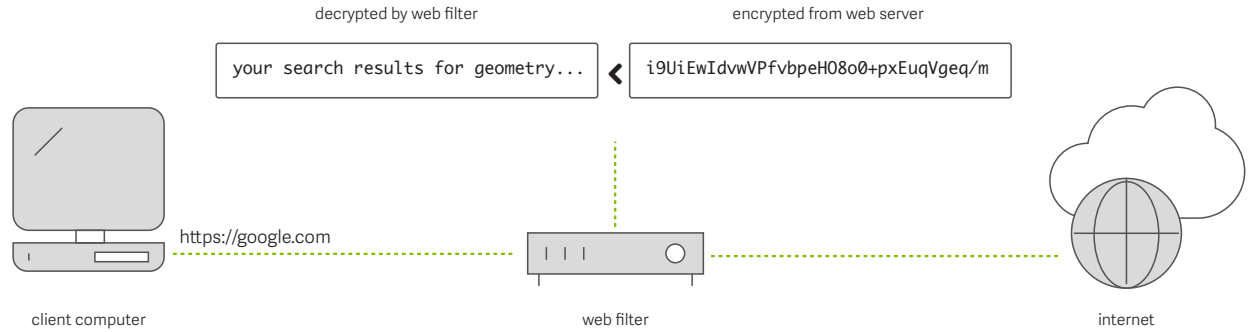


Figure 21

> For a school, a trusted man-in-the-middle approach is the only way to see exactly what is happening on the network.

Trusted Man-In-The-Middle Proxy

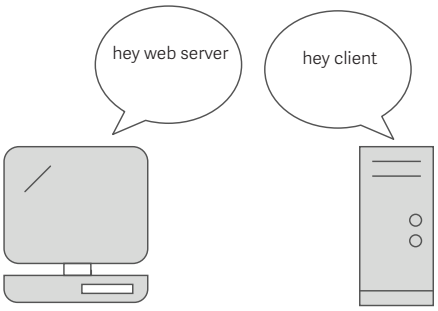


Figure 22 non proxy

Typically, a Web filter will be placed in a network in a non-proxy mode. This means that a client will not know the Web filter is there, and will make its requests directly to the Web server.

When a Web filter is configured to act as a proxy, the client knows that the Web filter is there, and asks the filter to make a request on its behalf. Then, the Web filter contacts the server.

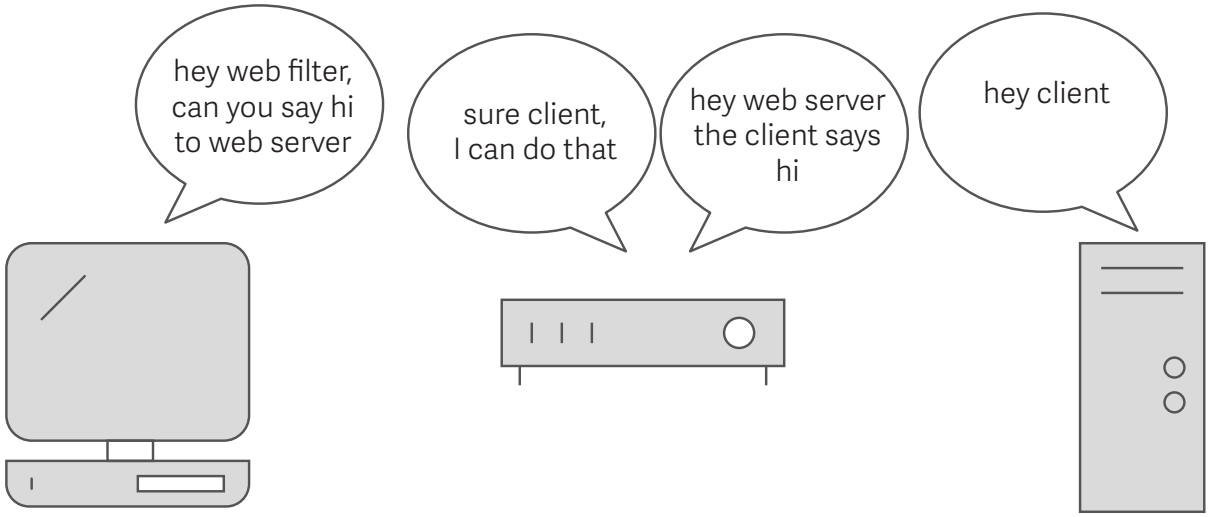


Figure 23 proxy

As previously mentioned, the client and server exchange data using an SSL certificate in order to encrypt/decrypt the data. In order to decrypt SSL traffic with a Web filter, your filter needs to be set up as a proxy. When the filter is acting as a trusted man-in-the-middle, the filter is an intermediary, intercepting the SSL certificate from the server and making its own SSL that matches and sends that new certificate to the client.

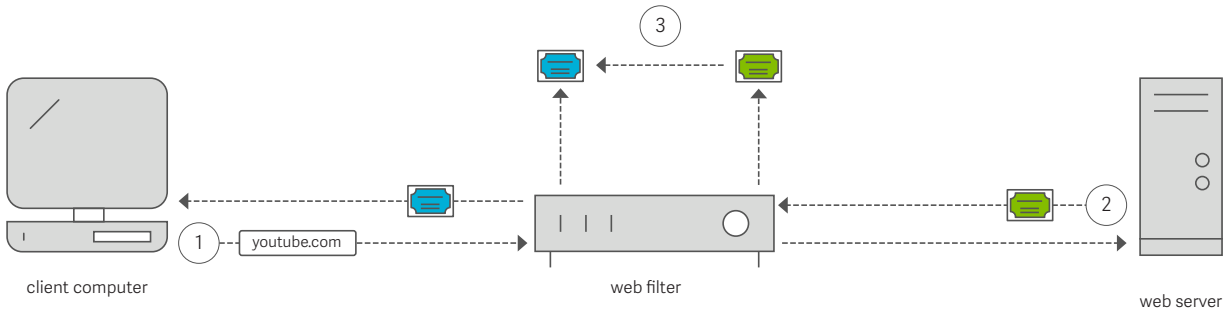


Figure 24

1. Client sends the request to the proxy, saying it wants to reach the web server. The web filter makes the request to the web server.
2. Web Server sends the SSL certificate. The web filter intercepts the certificate and creates its own certificate based off the web server's certificate.
3. The web filter sends the newly created SSL certificate to the client computer.

This gives the Web filter access to the encryption key so it can decrypt the traffic.

Essentially, these are the three main approaches for filtering SSL. You can combine methods from these various approaches to create a more ideal way of handling network traffic, but these three options are how Web filters handle SSL traffic

Lightspeed Systems Web Filter + SSL

By now, you understand what SSL is, how it works, and various methods for filtering SSL traffic. Let's examine how Lightspeed Systems Web Filter filters SSL.

To understand that, you need to understand a few key terms.

- Inline
- Proxy
- PAC File
- Root Certificates
- WCCP
- LS Web Filter Modes

What Does Inline Mean?

It's pretty simple: You can have a device "inline" or "out of line.

If the device is inline, the data flows through it when going from a client to a Web server. You can compare it to driving a car on the freeway from point A to point B — that freeway is inline.

In contrast, a device that is out of line is like a car on the freeway taking a pit stop for gas, then getting back onto the freeway to continue the journey.

What Is a PAC File?

PAC, or Proxy Auto Configuration, is a file that contains all the settings for what traffic goes to the proxy and what traffic doesn't. For instance, you can specify in your PAC file that www.mybank.com should not go through the proxy, but all Google traffic should. These files must be created by the network administrator. (Lightspeed does not create your PAC file because these settings vary so much based on schools' needs and preferences.) The PAC file is then downloaded to the client device/computer.

What Is a Root Certificate?

We've talked about SSL certificates, certificate authorities, and the idea of trust. A root certificate is basically a bank of trustworthy certificate authorities. Web browsers come installed with most of major companies' root certificates. However, because the Lightspeed Systems Rocket creates its own certificate, you need to add a root certificate to the client devices/computers so they trust Lightspeed.

What Is WCCP?

WCCP is a type of protocol used to handle decisions to send traffic to the Web filter in proxy mode, which basically bypasses the need to install the PAC file. (This is handy for BYOD programs.)

These are the most important concepts. Now, let's look at the Lightspeed Systems Web Filter.

The Lightspeed Systems Web Filter can be configured to operate in three modes:

- transparent bridge
- proxy
- firewall URL filtering

A transparent bridge configuration means that the Rocket is placed in line and acts like a bridge for the traffic to cross.

Proxy mode means that the Rocket is placed out of line and is acting as a proxy server. If you want to be able to decrypt SSL traffic, you need to be in proxy mode.

> School networks are all unique, and as such, Lightspeed has created a highly flexible Web filter that allows for the combination of many different settings and setups. For further help, please take a look at our community site. As always, feel free to contact us directly for support.

Firewall URL filtering is an out-of-line solution for larger networks in which the Web filter's primary role is that of a policy server.

In addition to these three modes, there are a few settings within the Rocket that affect how it handles SSL traffic.

Decode SSL

If you check this box, you can read the SSL certificate and see the domain that the client is trying to access.

Decrypt SSL

This allows you to decrypt the SSL session and see the full URL. (You have to be in proxy mode in order to use this option.)

This table helps you to see how each setting and mode works with SSL traffic.

Search query via YouTube: “newtons laws”

URL: https://www.youtube.com/results?search_query=newtons+laws

	Report View
Firewall URL Filtering	show IP address, e.g., 208.65.153.238
Transparent Bridge	show IP address, e.g., 208.65.153.238
Transparent Bridge (with decode SSL)	youtube.com (with SNI)
Proxy	youtube.com
Proxy (with decrypt SSL)	youtube.com/results?search_query=newtons+laws
Proxy (with WCCP)	youtube.com/results?search_query=newtons+laws

Lightspeed Systems

About Lightspeed Systems

Lightspeed Systems builds smart solutions for school networks

Since 1999, Lightspeed Systems has partnered with schools around the world to help them manage, secure, filter, and report on their school networks. All of our products are made just for schools with the features and services schools need. That's why our award-winning web filter, MDM, and classroom management solutions are happily used in more than 4,500 districts, making technology integration easy and safe for IT.

The Lightspeed Systems Rocket Web Filter can help you solve your SSL problems -- and a lot more.

Contact us:

www.lightspeedsystems.com

sales@lightspeedsystems.com

support@lightspeedsystems.com

1 877.447.6244