



Proxy Blocking: Preventing Tunnels Around Your Web Filter

Information Paper
August 2009

Table of Contents

Introduction	3
What Are Proxies?	3
Web Proxies	3
CGI Proxies	4
The Lightspeed Proxy-Blocking Method	4
Block unknown URLs	4
Block categorized domains and IP addresses of known proxies.....	4
Block unknown URLs matching proxy patterns	5
Block all proxied requests	5
Block SSL proxies.....	5
Block Ultra Surf connections.....	5
Block proxies at the desktop.....	5
A complete solution	6
Recommended Best Practices.....	6
Information	7
Communication.....	7
Additional Options to Implement	8
Lightspeed Solutions	9
Conclusion.....	9
About Lightspeed Systems.....	10

Introduction

Two thirds of respondents to Lightspeed Systems' survey, 2007's Top IT Headaches for K-12 Schools, indicated that proxies bypassing the Internet filter was a somewhat critical or critical issue. As proxies gain both new levels of sophistication and accessibility—and as students gain increased sophistication and desire to utilize those proxies to access blocked content—addressing the complex issue of proxy blocking is a top concern for school IT administrators.

What Are Proxies?

The most commonly reported tool to bypass Internet content filtering is the use of 'Proxies' to disguise browsing activities. Generally, a proxy simply acts on the user's behalf; accessing the desired websites (blocked or allowed) and discretely returning the content to the user while making it appear to be a benign or legitimate request.

There are multiple proxy options available to the enterprising user. Some are simple and easily recognized and managed; others are more complex and elusive to monitor and control. Newly "discovered" proxy options are eagerly shared through various Internet venues such as hacking and phishing websites, blogs, chatrooms, forums, and instant messages—and each "new" option is quickly adopted by a flurry of users just as eager to test them.

Since you can only enforce acceptable use policies on traffic you can see, recognizing and blocking such anonymizers is essential—and requires some very sophisticated software.

There are actually 2 basic types of proxies that are employed across the Internet: true web proxies (web and email proxy servers) and cgi proxies (scripts and programs that run on web servers and are invoked by users on the fly).

Web Proxies

True web proxies can be generally identified by their use of standard protocols to proxy web traffic.

Lightspeed Solution: These web proxies can and are being detected programmatically through the systematic processes of the Lightspeed Categorization Engine. When these are discovered, through the analysis of unknown URLs and the periodic re-evaluation of current content database entries, they are assigned to the 'Security.Proxy' category of the database. Most recently we launched a project to revisit every proxy site listed in the content database and "screen scrape" each page and link to make sure that all URLs are listed in the 'Security.Proxy' category. Over 700 additional proxy sites were initially identified and your local content database is being updated daily with these new entries as well as the refreshed entries. Subsequently, if you've chosen to block the 'Security.Proxy' category, your users will NOT be able to access the proxy websites that are allowing them to bypass your filtering and monitoring policies. Most web proxy servers that your users are able to find and experiment with, will still NOT return blocked category websites. The Content Filtering Object will recognize the actual target URL

address being requested through the proxy and will block access, as specified in your Content Categories policies.

Spammers also use web proxy servers to aid in the propagation of their spam mail campaigns.

Lightspeed Solution: Lightspeed is currently re-testing each IP Address listed in the database (over 1 million entries) to ferret out actual web proxy servers. This testing is quite time consuming and we have a battery of servers performing the process - similar to the 'Proxy Testing' actively performed by the Spam Mail Blocker - to help speed this evaluation. Though we believe we already have a fairly comprehensive listing of these sites due to this ongoing testing through our spam blocking process, we also believe that the end result of this project will be a dramatic increase of identified web proxy servers and a decrease of spam mail intrusions on your network.

CGI Proxies

CGI proxies are the most difficult to recognize and isolate because each one is done differently and requires more time intensive analysis to identify the web servers supporting the execution of the proxy CGI scripts and programs, which are routinely shared around the Internet.

Lightspeed Solution: Using our comprehensive analysis of identified proxy domains, we are developing a unique 'template' of common phrases and word-combinations that will help identify CGI proxy methods currently being employed and potentially being created. Armed with this model, we will, again, download and analyze every possible Internet website and update your database with the latest proxy listings.

The Lightspeed Proxy-Blocking Method

As proxy technology becomes more complex in attempts to anonymously tunnel users through content filters, Lightspeed Systems continues to develop new proxy-blocking methods to detect its presence and circumvent its processes.

Block unknown URLs

When a newly created site hits the Internet, no content filter has it categorized. It is "unknown." Not knowing if it's "safe to allow" is why many choose to block all unknown URLs, that is, block access to all URLs that are not in the database. Further, Lightspeed can be automatically notified of the new URL, which triggers an immediate review to categorize and add it to the content database. In turn, database updates are pushed out daily—or, for critical updates, every 30 minutes. This option to block unknown URLs can be enforced for all users, students only, or any group you define with separate policies.

Block categorized domains and IP addresses of known proxies

Proxy sites cannot hide from Lightspeed for long. Through Lightspeed's constant downloading of the entire Internet, proxy sites are easily detected and categorized accordingly. Further, Lightspeed customers submit new proxies every day. A scheduled task automatically forwards previously unknown

websites that users attempted accessing, and these are analyzed and categorized accordingly. The content database now includes more than 35 million categorized addresses and is open for review at <http://www.lightspeedsystems.com/Search>.

Block unknown URLs matching proxy patterns

A more direct, real-time approach to block proxies is to block all unknown URLs with matching proxy patterns. When a user attempts to access a site that is not in Lightspeed's content database, Total Traffic Control will search for signs of proxy activity using on-the-fly, deep-packet inspection. When a request matches one of the hard-coded patterns, Lightspeed blocks the request and logs the attempt. As proxy methods evolve, Lightspeed will continue to add patterns.

Proxy patterns is an optional setting, but Lightspeed highly recommends its use. If the broader "Block Unknown URLs" has been a source of over blocking on your network, Proxy Pattern Matching solves this by targeting proxy requests specifically. With a click of the button, you can stop new proxy sites cold in their tracks. When enabled, the content filter will inspect every unknown web request for matching results. When a request matches one of the hard-coded patterns, TTC blocks the request and displays "The requested page has been blocked by the content filter because it is not a known website that has been categorized, and it matches a proxy pattern." TTC logs these attempts in the Blocked Content report as "Match Proxy Pattern." As proxy methods evolve, Lightspeed will continue to add patterns. If you come across new and unknown proxies which seem unaffected by this feature, please let us know, so we can add it to the arsenal.

Block all proxied requests

By choosing to block all proxied requests, you can prevent access to the Internet if a web request is using any proxy server. For instance, if a user configures his browser to use either a local or external proxy server, all web requests will be immediately blocked, regardless of destination. Any third-party browser plug-ins designed to utilize the browser's proxy settings will also be blocked.

Block SSL proxies

With SSL Proxy Blocking, you can filter any SSL session in the same way as non-secure web sessions. The Total Traffic Control server will perform domain name categorization and policy lookups, and apply the non-secure session policy options (such as blocking unknown URLs, workstation overrides, and the allowed & blocked web site URL lists). With four levels of SSL Proxy Blocking (None, Low, Medium, and High), you can choose the level of security for SSL sessions that meets your needs. The level you select determines what is used to perform database lookups, i.e., domain or IP, for the SSL request.

Block Ultra Surf connections

When SSL Proxy Blocking is set to High, you have the additional option of blocking all Ultra Surf connections. With this option, we will specifically target sessions that are using UltraSurf's SSL signature (including v8.9+) and block them.

Block proxies at the desktop

Finally, desktops with Lightspeed Security Manager installed can stop proxies in two additional ways—

through Lightspeed-distributed signatures that identify the proxy service application as a virus and by disabling read/write access to removable media. Lightspeed Systems maintains a comprehensive database of virus, spyware, and malware signatures—and distributes signature updates to you every day, and emergency updates immediately. Also, unique file IDs of each valid program on your network make changes to programs (such as by a virus) immediately recognized, treating the altered file as an “unknown program” with your specified permissions/restrictions.

A complete solution

Together, these methods offer a complete proxy-blocking solution:

- If you block the Security.proxy category, users cannot, for example, get to UltraReach.com and download UltraSurf. (Note: You can also block users from searching for the words UltraSurf or UltraReach.)
- If you block unknown URLs, users can't access a copy of a proxy program that's been stored on a new site.
- If you check unknown URLs on the fly, users can't access sites that come up positive for proxy activity.
- If you block all proxied requests, you can prevent access to the Internet whenever a web request is using a proxy server.
- If you set SSL proxy blocking to High, all SSL communications will be validated and those without a legitimate certificate will be blocked.
- If you enable Ultra Surf blocking, any SSL session that uses Ultra Surf's signature will be blocked.
- If you configure the Security Agent to disable read/write access to removable media, you can stop a user who brings a proxy in on a thumb drive.
- If you use the Security Agent, a downloaded proxy will be stopped from running with a virus signature supplied by Lightspeed.

Lightspeed also offers the flexibility to implement these proxy-blocking methods differently for different users or groups. With these defenses in place, you can win the proxy battle.

Recommended Best Practices

The dynamics of the Internet combined with the nature of some users (inside and outside of your network) to repeatedly experiment with new ways to "break the rules", require that proxy blocking be an ongoing exercise.

Your best weapons in this battle are information and communication.

Information

Use your TTC traffic reports to help you identify the potentially "inappropriate" activity.

The '*Unknown URLs*' report will usually be your first indication of an industrious user lurking into areas that they shouldn't. You can use this report to personally evaluate unknown websites and directly categorize them into your local database, but these unknown URLs are also automatically sent to the Lightspeed database manager for evaluation and addition to the master database which will be updated back to your location. This monitoring, used in conjunction with a policy to "Block all unknown URLs" will restrict users from finding and using - or even creating - new domains to use as proxy tools.

The '*Busiest Protocols*' report can point out an undue increase of "https" traffic that may be signaling the use of SSL links to proxies, which may warrant a more in depth look at what the associated users are REALLY doing.

The '*External URL Hits*' report may show excessive activity related to specific users or specific websites, again warranting a bit more investigation.

The '*Lightspeed Internet Archive*' can help you quickly evaluate a website or its linked websites and determine its nature and justification for activity on your network.

Comments, observations and feedback from "the field" can give you information about activity observed first hand (from teachers or administrators), and sometimes, what "chatter" can be picked up that may give away a "new" circumvention method that is being used.

Communication

Share your observations and discoveries with Lightspeed to help us build our proxy-blocking arsenal. When a new method of defeating your system policies and procedures has been discovered, simply send a descriptive message to the Lightspeed database manager at content@lightspeedsystems.com. An offending address can be quickly evaluated and added to the database for the benefit of ALL TTC installations. Conversely, as our database management team works back through the database, it is expected that some legitimate web sites, mostly related to the 'Computer' category, may be temporarily mis-categorized into the 'Security.Proxy' category, until they can be verified through secondary tests and evaluations. Using the "Blocked for Review" process you can help us correct these over-blocked situations and better refine the analysis process. If you discern a pattern of over-blocking, please let the database manager know immediately.

Additionally, any spam items that defeat or make it past the Spam Mail Blocker should be forwarded to spam@lightspeedsystems.com by all of your users. Simply use the 'Forward' option of your email desktop client to copy the offending item to us so that we may evaluate the source and content of the suspect email. This will help us identify new spam sources or methods which will, in turn, allow us to enhance spam blocking AND improve web proxy listings.

Additional Options to Implement

Take advantage of the built-in tools that Total Traffic Control provides:

Block the Proxy Category: Set the blocking status of the 'Security.Proxy' category to "BLOCKED".

Block access to Unknown URLs: With the TTC content database currently listing over 35 million Internet domains and websites - and hundreds of new sites being categorized and added daily - it will be the rare circumstance that users will be connecting to legitimate unknown websites. By blocking unknown URLs, you immediately eliminate access to potentially negative websites until they can be evaluated, categorized and added to the database. With evaluation and categorization of unknown websites occurring nightly (locally and/or through the Lightspeed master database), by the time the user alerts your staff, and/or the Lightspeed staff, to the over-blocking issue, the database will have been appropriately updated.

Block Non-http traffic to blocked IP Addresses: Traditional 'Proxy' websites are accessed through an http link to a sever that provides and maintains a connection to the user's target websites. These proxy sites are known and categorized into the '**security. proxy**' category and are easily blocked by a category setting in a policy. But an alternative ploy is to establish a link to these servers using a secure interface - SSL or 'HTTPS' - to encrypt the communication. The encrypted session requests cannot be analyzed to determine their target destination, so this kind of proxy connection must be stopped by limiting the HTTPS requests when the request is targeting an IP Address (proxy server) that is in a blocked category, such as the 'security.proxy' category. By setting your Content Filter global properties to "*Block non-HTTP Traffic to Blocked IP Addresses*" SSL connections to known proxy servers or other blocked category IP addresses will be blocked.

Remove N2H2 and Websense Content Proxy support: In some TTC networks, it was desired to maintain N2H2 and Websense content servers alongside the TTC Security Server. In order for these agents to operate cooperatively, specific TCP ports were assigned to handling traffic between the devices and to bypass the TTC Content Filter. When N2H2 or Websense content servers are NOT employed in the network, these ports become open paths that can be used to address HTTP proxy requests to proxy sites and bypass Content Filtering policies. If you are NOT integrating N2H2 or Websense servers within your TTC network, you should modify the unique TTC Content Filter registry key and close the associated ports.

Verify the automatic Unknown URL Reporting: You should systematically copy and send any unknown URLs that your users encounter to the Lightspeed database manager so they can be evaluated and added to the master database. This process should be enabled as a *Scheduled Task*.

Test for Proxy Servers: You can use the Spam Mail Blocker to do additional real-time testing of unknown mail servers to determine if they are Proxy servers or open relay services.

Monitor and Report Internet Traffic by Internal IP Addresses: It is important to make sure that your TTC Server is appropriately capturing the data that will help you track user activity by setting up the Traffic Classification Object properties to record traffic by "URLs for Internal IP Addresses."

Closing the proxy loopholes to and from your network may continue being an unfinished task, but it's one that Lightspeed Systems will unfailingly continue to address.

Lightspeed Solutions

Total Traffic Control is the complete solution for managing your school network's usage, health, and security. With this comprehensive solution you can monitor user activity, ensure Acceptable Use Policies are being followed (on email, the Web, or the desktop—both on the network and off), reduce dangerous and costly security threats, ensure school resources are utilized safely and effectively, and easily view and share critical information with custom reports.

Components of Total Traffic Control (available as part of the comprehensive solution or as individual components), which are vital to the proxy blocking process:

Web Access Manager delivers safe and appropriate web surfing for all users with customizable filtering. It utilizes multiple layers of anonymous proxy detection and blocking to keep users from bypassing your filter and accessing blocked sites.

Security Manager eliminates threats from viruses, spyware, and malware with desktop and gateway security. It provides application-level proxies for many protocols, including HTTP, FTP, and SMTP, give you the ability to allow or deny specific commands within these protocols at the gateway level.

Email Manager archives, reports on, and manages communications, while controlling spam and viruses. Its spam mail blocker delivers real-time testing of mail servers to see if they are proxy servers.

Conclusion

The fight against proxy tunnels is ongoing, but it is critical to the safety of students, the enforcement of Acceptable Use Policies, and the security of your network.

Lightspeed is committed to developing innovative methods to identify and block proxies. Total Traffic Control content database has over 35 million identified and categorized domains and IP addresses, and is being updated daily with new categorized web sites.

In addition to our ongoing efforts to block proxies through our filtering database, Total Traffic Control reports can help isolate patterns and locations of abuse and network misuse.

And, always share your discoveries, suspicions, observations or concerns regarding network incursions to our Database Manager at content@lightspeedsystems.com . This information is vital to our ongoing commitment to help you stay in control of your network.

About Lightspeed Systems

Lightspeed Systems Inc., founded in 2000, develops comprehensive network security and management solutions for the education market. We are committed to helping schools operate their networks effectively and efficiently, so educators can provide safe online teaching and learning environments.

Our software is used in more than 1,000 school districts in the United States, the United Kingdom, and Australia to protect more than 5 million students. For the past two years, Lightspeed Systems has been recognized on the Inc. 5,000 list as one of the fastest-growing private companies.

www.lightspeedsystems.com