Shadow Surfing
Preventing Proxy Abuse in Schools

What are Anonymous Proxies?

Circumventors, shadow surfing, anonymizers, proxy avoidance – call them what you will, anonymous proxies have been with us for about as long as we've been filtering the web.

What they provide is simple – online anonymity. This may be a lifeline for political dissidents in countries where censorship is a problem but it is also a major problem for organizations who need to control and monitor their users' web access.

In basic terms, anonymous proxies are simply proxy servers - they pass users' web requests onto other servers on the Internet. They help users to sidestep security by allowing them to browse secretly through them – and view banned online content within them - without disclosing the URLs they visit to filtering products.

Why is Proxy Abuse a Problem?

There are now millions of proxies in existence with miscreants changing URLs and developing new techniques far faster than security vendors can hope to block them.

The proliferation of proxies is already well beyond the control of URL based filtering products and although keyword-based filters will catch sites with 'proxy' in the title, many have legitimate-sounding names.

It only takes one proxy to put a gaping hole in your network security. Using a web filtering solution that doesn't block proxies is the equivalent of putting a big bolt on your front door but leaving the back door wide open.

How do students know/find out about proxies?

As with most things, the first port of call is the web. Try entering "unblock facebook" into Google – the results run to millions of sites, all offering the same thing – anonymous browsing.

'Backdoor' URLs are passed quickly from student to student with some proxy sites even offering to send daily updates on the newest and hottest proxy sites via email or text message.

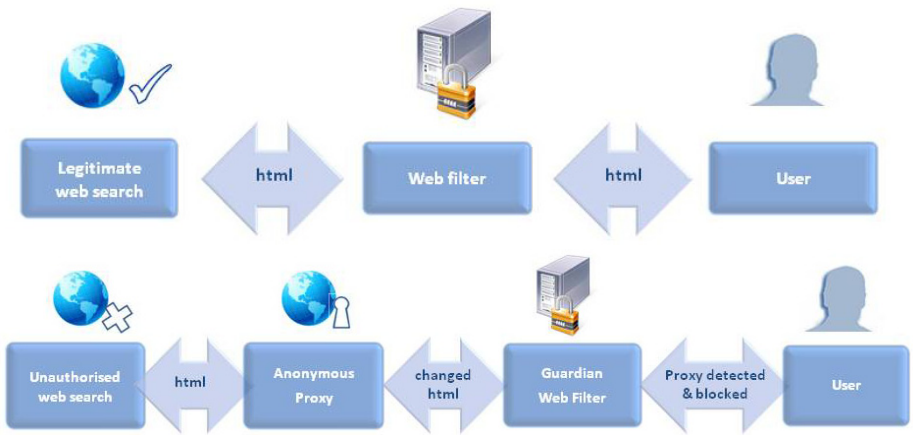
There are also plenty of step by step videos on YouTube showing students how they can use proxy tools to bypass school filters. These are the very skills that we don't want our children to learn in school – digital lockpicking and worldwide web breaking and entering.

Different types of proxy and how to defend against them:

Web-based Proxies

Web-based proxies work entirely through a web browser and use server-side software such as CGIProxy, Glype, PHProxy and other custom scripts. All users need do to use these sites to surf anonymously is enter the web addresses they wish to browse to in the box provided (usually on the home page).

URL or keyword-based filters may block some of these but the only way to reliably prevent access is to employ an intelligent filter that is capable of detecting – and accurately blocking the characteristic signatures or patterns of proxies, as the diagrams below demonstrate.



Open Proxies

SSL proxies use HTTPS connections which allow users to secretly view illicit material (including media files) within a secure tunnel where content is encrypted. URLs visited via SSL proxies don't appear on logs and so IT staff are often unaware of the extent of their problems with the secure variety of these proxy pests.

URL and keyword based filters are an utterly futile defense against SSL proxies. Even some so-called 'third-generation' filters aren't intelligent enough to provide proper protection. Some offer the option of blanket blocks on all HTTPS traffic – but this is far from practical in an office environment. A whitelist of authorized HTTPS sites is a better option but will still result in over-blocking complaints, due to the sheer number of sites now using SSL encryption. (Over 2 million sites now use SSL including some popular webmail and IM services such as Hotmail, Gmail and GoogleTalk).

To accurately defend against SSL proxies, filters need to be capable of inspecting and validating SSL certificates (few proxies have valid ones) and ideally decrypting and inspecting all incoming and outgoing HTTPS traffic, to make signature and content-based filtering possible again.

Proxy Networks (e.g. TOR)

Various proxy networks exist (TOR is the best known example) that use layered encryption (also called "onion routing") and peer-to-peer networking to allow their users to communicate anonymously with each other. Most rely on end-users to donate bandwidth and other resources to the network. Because the servers used are not controlled, some are operated by malicious individuals – who use them to distribute malware and other web nasties and intercept traffic.

To defend against the use of proxy networks requires a combination of firewall rules, web filtering rules and local policy settings.

Proxy Software Applications

Some subscription-based services offer client-side application software to automatically configure your browser's proxy settings. Most are simply open proxies dressed up with a fancy interface but some use HTTPS connections to outwit less intelligent filters and are hence becoming popular options for students.

One of the most popularly used applications (Ultrasurf) is a free 100kb download. Blocking downloads and denying installation rights to anyone but administrators helps to prevent their use. Several of the prevention methods listed above for other types of proxies also work on application-based proxy tools.

Who makes proxies and why?

Proxies require a lot of bandwidth to host. This bandwidth costs money, sometimes quite a lot. So who is hosting these proxies, and who is footing the bill?

A few proxies are hosted by technically-adept students, bypassing their school filters, and limiting the use to a select group of their peers. Frequently these types of proxy are hosted on a home broadband connection, but with a handful of users, that's no problem. These are the only truly 'free' forms of proxy and they can also be pretty tricky to block – URL list-based filters will almost never catch them!

Public web proxies on the other hand (the most common type) can eat their way through many gigabits of bandwidth. The cost of this is usually offset by placing pay per click adverts on the proxy page. Revenue is miniscule, but with many hits, it all adds up. Of course, the proxy owners have to advertise too – top proxy lists are one way of doing this, but sometimes legitimate ads are placed as well.

Some software-based proxies charge a fee but the majority are free and don't carry any ads. Since it is highly unlikely that the creators are magnanimously footing the hosting bills, these proxy services will undoubtedly be selling on browsing habits, injecting ads or unwanted text, and even pushing malware.

Proxy abuse - what are the risks?

Legal risks

Internet security standards at a school in the UK were recently exposed on the BBC news after the mother of one young boy complained that her son had returned home with a printout of a pornographic image obtained via school computers. The head was forced to send letters home to all parents regarding the matter and suspend Internet use until the security standards were improved. Although schools are not yet facing lawsuits for security breaches of this type, it is only a matter of time before a protective parent decides to prosecute.

In the US, schools must comply with the Children's Internet Protection Act (CIPA), a federal law enacted by Congress in 2000 to protect children using school, college and library computers from offensive Internet content. All obscene, harmful and pornographic content must be blocked and all student web use monitored.

Institutions that fail to comply risk losing e-rate funding (special Government discounts designed to make telecommunications and Internet access more affordable for schools).

Cyberbullying

Anonymous proxies are also popular with cyberbullies, who need them to cover
their tracks so they can taunt teachers and students with impunity. Proxy tools help them to keep their online activities off the radar so they can remain unidentifiable and escape punishment.

Malware

Not only do proxy sites give users unfettered access to the content you are attempting to block, they also help malware and other web-related threats to sneak into networks undetected. SSL proxies are a particular problem since the secure tunnels used allow viruses and worms to sidestep network anti-virus and web
filtering security entirely.

Phishing and password theft

Many proxy users are also unaware of the risks to their own personal security and identity. Malicious proxy servers do exist and are capable of recording everything sent to the proxy, including unencrypted logins and passwords. Although some proxy networks claim to only use 'safe' servers, due to the 'anonymous' nature of these tools, proxy server safety is impossible to police. Users should be educated to understand that whenever they use a proxy, they risk someone "in the middle" reading their data.

How Guardian prevents proxy abuse

Many vendors block proxies by simply restricting users to a whitelist of URLs which frequently results in overblocking.

Instead of relying on whitelists, Guardian uses Dynamic Content Analysis to screen all requested web pages for the tell-tale signatures of proxies. This technology examines the content, context and construction of web pages in real time so that proxies and other malicious or undesirable material can be accurately identified, classified and blocked. SSL Interception also ensures that filtering (and Dynamic Content Analysis) is performed on all traffic that utilizes secure or https connections, preventing SSL proxies with valid SSL certificates from slipping through the net.

Thanks to this intelligent technology, and our development team's ongoing commitment to ensure that detection signatures are constantly kept up to date, Guardian has an excellent proxy-blocking record. In the last 18 months, the number of types of proxy we detect has quadrupled and this figure will continue to grow as new proxy technologies and variants of existing proxies evolve.

Guardian's URL blocklists (which provide a secondary defence mechanism) are also updated on a daily basis with newly discovered proxy URLs.

Other tips to prevent proxy abuse

- Educate teachers to recognise illicit surfing or proxy abuse and report it to the IT department
- Educate students about the danger of using proxies.
- Allow slightly more lenient filtering outside of core hours
- Make sure your AUP covers anonymous proxying and that both students and teachers are familiar with its content. Make it clear that proxy abuse can be tracked to individuals

Conclusion

Proxy abuse is an increasingly pervasive problem – and one that can only be prevented with intelligent filtering solutions such as Guardian. Smoothwall's pioneering Dynamic Content Analysis technology was developed in 2001 (several years before most other vendors) and over the last 6 years has been extensively refined to maintain accuracy and eliminate over-blocking. Smoothwall filtering solutions are also Becta-accredited, which proves that they meet the UK Government's rigorous standards for filtering products used in education.

UK + INTERNATIONAL

Smoothwall Ltd
1 John Charles Way
Leeds LS12 6QA
United Kingdom

+44 (0)800 5 999 040 UK
+44 (0)870 1 999 500 International
sales@smoothwall.net
www.smoothwall.net

USA + CANADA

Smoothwall Inc.
6201 Fairview Road, Suite 320
Charlotte, NC 28210-4274
United States of America

1-800-959-3760 US + Canada
1-888-899-9164 Fax
sales@smoothwall.com
www.smoothwall.com