



Web-Based Proxies: Today's Leading Threat to Internet-Assisted Learning

INTRODUCTION

District IT administrators are very familiar with the negative impact Web-based proxies are having on maintaining a safe learning environment for students. Today there are tens of thousands of Web-based proxies on the Internet with more becoming available every day. As their primary source to getting around Web filters, students freely utilize Web proxies — also known as proxy anonymizers — unaware of the dangers they present to both students and schools.

Five years ago proxy sites were few and far-between. So what has happened since then? Web-base proxies have increased exponentially, dramatically impacting child safety in schools. The reason for the drastic increase? Software running on proxy anonymizer sites has gone open-source making Web-based proxies available for free to anyone that wants to access them. This new open-source approach gives non-tech savvy students the ability to create Web-based proxies on the fly. These proxies are then placed on newly created Web sites, often bypassing Internet filters, because these sites are uncategorized.

This white paper examines Web-based proxies, the threat they pose to educational organizations, and explains how IT administrators can protect schools by implementing a filtering solution that eliminates proxy access in their district.

HOW WEB-BASED PROXIES WORK

Web proxies are probably the most popular and successful way students bypass Internet filters today. Appearing as an unblocked Web page, a proxy anonymizer site allows a student to enter a URL address using a form that, when submitted, causes the proxy server to retrieve the web page despite being blocked by the school's Internet filter.

It is the cryptic nature of Web-based proxies that poses a significant challenge in education, because it allows students to access inappropriate and potentially harmful sites prohibited by their schools' Acceptable Use Policy (AUP) and the Children's Internet Protection Act (CIPA). By hiding IP addresses and information such as students' Web histories, proxy anonymizers prevent most Web filters from monitoring what students are viewing online. For example, students trying to access blocked sites such as MySpace.com oftentimes configure their home computers as proxy servers, allowing them to "tunnel" into their proxies to access the site.

Jim Culbert, Information Security Analyst for Duvall County Public Schools (FL), knows all about the danger proxies bring to educational institutions. His own experience started with MySpace.com — a Web site all too familiar to students as well as staff. In this particular case, Mr. Culbert noticed a massive rise in proxy server activity since he blocked the social networking site from being accessed in his district. He tracked the proxy activity and rounded up the most active student users. Certain they were after obscene material on the Web, he was surprised that they were just trying to access their MySpace e-mail accounts. Because the site was blocked, students were utilizing proxies in order to access it. Although the students were considered the brightest in their school, they had no idea that information such as their usernames and passwords were retrievable by unknown proxy administrators, many of whom are hackers. These same hackers write proxy programs that can get into a school network and do millions of dollars in damage.

WHY MOST FILTERS DO NOT EFFECTIVELY BLOCK WEB-BASED PROXIES

The open-source community has made it so a technical novice can start a proxy anonymizer site. A simple search of blog sites such as MySpace.com or LiveJournal.com will show a plethora of pages that instruct a student on how to bypass his or her school's Internet filter. All the student needs is a Web server and proxy anonymizer software, both of which are freely available from many different sources on the Internet. Once the student has uploaded the software to the Web server, that student and his or her friends can bypass the filter. Word travels, and soon students from other schools across the country are using a simply designed proxy anonymizer to bypass the most complex Web filter.

For example, in 2005 a high school sophomore made the front-page news when it was discovered he had provided two months of unfiltered Internet access to his peers through a proxy anonymizer site he created. Over 2,000 hits were registered to the site, which students used to access anything from research to adult sites. This is not a lone case — an increasing number of school districts are being placed in the limelight for failing to prevent these mishaps. Although most Internet filtering solutions include a "Web-Based Proxy" category in their databases, they actually fail at blocking access to Web-based proxies due to their "list-based" approach. Unfortunately their "list-based" database cannot keep up with the increasing number of new proxy sites, making it extremely easy for students to access proxy anonymizers and causing additional problems for overburdened IT staff.

ADDRESSING THE CHALLENGES OF ANONYMOUS PROXIES

Internet Acceptable Use Policy

The first step an IT administrator should take to ensure a secure learning environment is to review their school's Internet Acceptable Use Policy (AUP). The AUP is the single most important part of governing what a student can access on the Internet. Even if a school already has an AUP in place, it is wise to review it and ensure that it clearly forbids the use of any technology designed to circumvent, avoid or bypass any network security controls. This includes Internet filters, anti-virus solutions or firewalls.

Schools must warn students they will be disciplined for violating the AUP and follow through with such discipline. Students should be aware violations of the AUP might result in loss of access to the Internet as well as other disciplinary or legal action. The intent of the enforcement is to change Internet behavior habits and steer students to educational-focused content.

Internet Filters

The second step an IT administrator should take is to evaluate the effectiveness of their current Internet filtering solution in blocking Web-based proxy sites. The most effective way to detect and block Web-based proxies is by implementing "signature-based" blocking technology in addition to just filtering by URL ("list-based"). This method of blocking examines data streams at the packet-level identifying patterns (signatures) associated with proxy anonymizers.

M86 is the only Internet content filtering provider that currently uses "signature-based" blocking technology in order to block peer-to-peer, instant messaging and anonymous proxies. Utilizing revolutionary Intelligent Footprint Technology™ (IFT), M86's R3000 Internet Filter or ProxyBlocker's unique "Proxy Pattern Blocking" catches requests for anonymous proxies on the fly, giving school districts zero-day protection against many open-source proxies. Therefore, if the site is not categorized as Web-Based/Anonymous Proxies in the M86 Database, the R3000 or ProxyBlocker will still block access to the site based on the signature files in the M86 database. This allows network administrators to immediately identify new proxy anonymizer sites when they are created, rather than days or weeks later when they are added to the URL list. In addition, the "Proxy Pattern Blocking" feature identifies attempts to set up proxy tunnels, prevents these connections from being made and keeps a record of the number of times a student tries to circumvent the filter in this way. After a predetermined number of attempts, the student is then denied Internet access.

SUMMARY

Web-based proxies are today's leading threat to Internet-assisted learning. Over-zealous students bent on circumventing the system, combined with an ineffective filtering solution, makes it next to impossible for overburdened IT staff to address this threat. Only through implementation of an Internet filtering solution that effectively blocks Web-based proxies, supported by an enforced Acceptable Use Policy, can districts and schools secure the learning environment.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters

828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific

Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Auckland, New Zealand

Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 09.01.09