

*Technology White Paper*



***The Quandary of Web Anonymizers***



## ***The Quandary of Web Anonymizers***

This white paper is written especially for executives and human resources, security and IT professionals. It explores the dangers of anonymous Web surfing within organizations and the use of anonymizing technologies and tools to circumvent existing Web filtering solutions and anonymously bypass Internet safety policies. This white paper will present the shortcomings of existing URL filtering solutions in protecting against the use of anonymizers and describe how a multi-layered, real-time Web security solution can more effectively and dynamically block this emerging threat.

# Table of Contents

The Quandary of Web Anonymizers .....	<b>1</b>
What are Anonymizers? .....	<b>3</b>
Covering Tracks – How do Anonymizers Work? .....	<b>4</b>
How Web Surfing Causes Trouble For Your Organization .....	<b>4</b>
The Malicious Aspect .....	<b>5</b>
The Compliance Aspect .....	<b>5</b>
Threats Posed by Anonymizers .....	<b>6</b>
Why Content Filtering Provides Only Limited Protection .....	<b>6</b>
The eSafe Multi-layered Solution .....	<b>7</b>
Layer 1 – URL Filter .....	<b>7</b>
Layer 2 – Protocol Filter .....	<b>8</b>
Layer 3 – HTTPS/SSL Inspection .....	<b>8</b>
Summary .....	<b>8</b>

# What are Anonymizers?

“Anonymizers” is a collective term referring to various tools and online services that commonly integrate proxy technologies to conceal a user’s Web activities. Initially, anonymizers emerged as “Anonymous Proxy Servers” designed to keep user activity on the Web private, and to avoid various “Internet censorship” initiatives. In the past few years, anonymizing technologies have grown to become a frequent and serious risk factor to both corporations and educational organizations.

The past year witnessed a drastic increase in the number of anonymizing services. This phenomenon, which started in 2002 with only a few dozen sites offering users anonymous access to Internet resources, has increased exponentially, especially over the past year. More than 100,000 registered Web sites and an estimated 300,000 home-based private Web sites now offer anonymity services.

There are two main reasons for this drastic increase. User demand for anonymous surfing capabilities created new opportunities for Internet entrepreneurs to sell anonymizing services, usually at a monthly or yearly fee, or to earn money through sponsored advertising via the service. The second reason for the increase is directly related to the availability of anonymizing technology. Software running on proxy anonymizer sites was widely promoted in the open-source community, making Web-based proxy software available at no cost to developers, and providing almost anyone with basic technical expertise the ability to create their own anonymous proxy in just a few hours. These proxies can be placed in hosting services or even on a PC at home, and accessed from anywhere on the Internet, including from within businesses and organizations equipped with firewalls and other security measures. Once accessed, they enable users to bypass existing Internet filters.

There are several types of anonymizers that exist today – commercial, non-commercial and home-brewed:

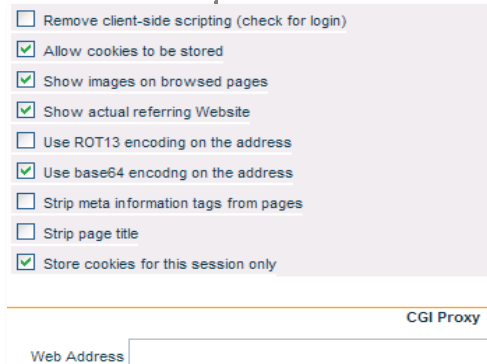
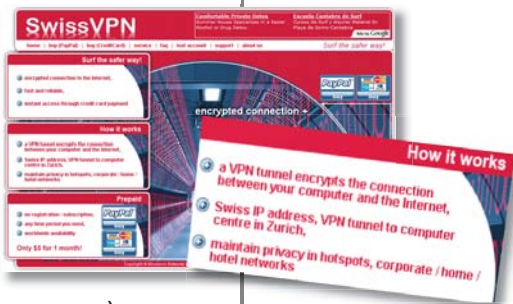
**Commercial** anonymizers charge subscription fees and usually provide high quality support services. One such example is the SwissVPN ([www.swissvpn.net](http://www.swissvpn.net)) that charges \$5 per month and provides an encrypted anonymous VPN channel from a user’s PC to a computer center in Zurich through which anonymous Internet surfing is available.

**Non-commercial** anonymizers do not charge any fee and usually generate their revenues from advertising to surfers that use their services. One such example is FreeProxy ([www.freeproxy.ca](http://www.freeproxy.ca)), a Canadian Web site that is actually a portal to other non-commercial anonymous proxies, ranking them according to availability and speed and allowing anonymous browsing through any of them.

**Home-brewed** anonymizers use one of the free and widely available open source anonymous proxy packages. Anyone with basic technical knowledge can download, install and operate an anonymous proxy at home. This method is very popular among high school and college students who use home-brewed anonymizers to circumvent existing URL filtering solutions and browse restricted Web sites using school computers.

The open source proxies are feature-rich and usually provide additional security options such as removal of scripts, cookies and meta-information.

Several of Aladdin’s educational institution customers reported that using eSafe, they have identified and successfully blocked students attempting to use open source anonymizers installed at their homes to browse to pornographic Web sites.



## Covering Tracks – How do Anonymizers Work?

Anonymizing tools are probably the most popular and successful way for users to bypass Internet URL filters. Appearing as an unblocked Web page, an anonymizer site allows users 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 organization's Internet filter.

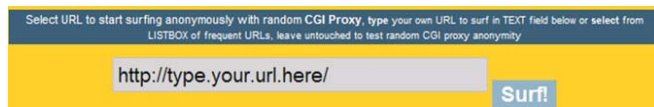
Access to open-source anonymizing tools is based on two main methods:

- **CGI-Proxy:** Users can use a CGI Script to retrieve any resource that is accessible from the server on which it runs. When an HTML resource is retrieved, it is modified so that all links in it refer back to the same proxy, including images and form submissions. Configurable options include text-only support, SSL support, selective cookie and script removal, simple ad filtering, access restriction by server, and custom encoding of target URLs and cookies.
- **PHP-Proxy:** A Web HTTP proxy programmed in PHP that can be easily installed on any PHP-enabled Web server. It allows users to browse through the Web server itself as a proxy for bypassing firewalls and other content filter restrictions. PHP-Proxy uses a Web interface very similar to the popular CGI-Proxy.

### Lozdodge v1

#### Lozdodge will allow you to avoid all Website filters

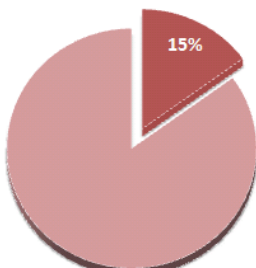
Download and install Lozdodge to an uncensored PC (like your home PC, for example). Lozdodge will then automatically host a proxy avoidance Website from the PC that it has been installed onto.



## How Web Surfing Causes Trouble for your Organization

An independent survey commissioned by Aladdin Knowledge Systems was conducted to determine the prevalence of anonymous proxies in U.S. workplaces. The survey asked U.S. workers a variety of questions surrounding their Internet restrictions at work, and their knowledge of anonymous proxies.

Anonymizers usage in organizations

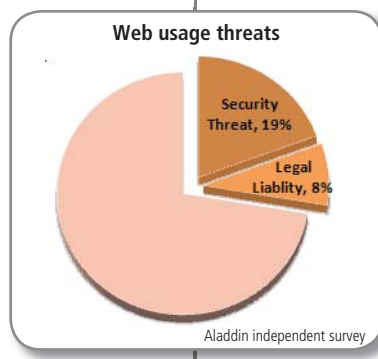


Aladdin independent survey

Among the most notable statistics in this survey were that more than 12 percent of workers in companies with 100,000+ employees said they have used anonymous proxy services to bypass corporate Internet security policies. Further, approximately 7 percent of employees across all sizes of organizations admitted to personally using anonymizers that enable them to circumvent Internet restrictions instituted by their company. In addition, 15 percent of those surveyed reported that they are aware of another person within the organization who bypasses corporate restrictions and visits blocked Web sites using an anonymizer.

Business & Legal Reports noted in their latest publication that “productivity concern is righteous, but it’s the least of the damage that uncontrolled Web use can cause an employer”. According to this research, the most serious consequences of uncontrolled Web use are employer legal liability and compromised security.

In a recent survey of more than 10,500 employees in seven major industry categories, it was identified that 8.23 percent of personal Web surfing posed the risk of legal liability and 19.42 percent posed a security threat to corporate networks. Accessed sites that carried these risks included personal dating, pornography, and gambling sites, anonymizers used to disguise one's ISP address so recipients can't see where messages originate, sites regarding weapons, hate speech, cults and the occult, and criminal skills sites. The primary threat posed by this kind of activity is that employees visiting these high risk sites are able to introduce spyware and malicious code into the corporate network. Even the industry with the lowest incidence rate, health care, still experienced 17.8 percent of its overall malware incidents from employee Web use.

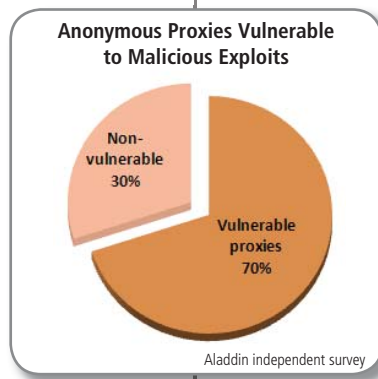


## The Malicious Aspect

Analysis of publicly available anonymizers found that 5% of these servers contained malicious content. Anonymous proxy servers contained infected files such as Trojans, script viruses and exploits, spyware, and adware on server directories.

A vulnerability analysis carried out by Aladdin's Content Security Research Team (CSRT) on 1000 registered anonymizing Web sites revealed that 70% of these sites are vulnerable to remote code execution and cross site scripting attacks.

Aladdin CSRT has also established that more than 90% of pornographic Web sites carry malicious content.



## The Compliance Aspect



Almost all the regulations that deal with information security address the issue of Internet safety policy. Most notable is CIPA (Children's Internet Protection Act) that was passed by U.S. Congress in December of 2000. CIPA requires both schools and public libraries to have in place and enforce Internet Safety Policies that address:

- Access by minors to inappropriate matter on the Internet
- Safety and security of minors when using electronic communication
- Unauthorized access including "hacking" and other unlawful activities by minors online
- Unauthorized disclosure, use and dissemination of personal information regarding minors

As part of CIPA enforcement, there have been several instances that teachers were held personally and legally liable for allowing children to view unsuitable content on schools computers.



Section 404 of the Public Company Accounting Reform and Investor Protection Act of 2002, commonly called Sarbanes-Oxley or SOX, addresses Internal Controls. Section 404 of Sarbanes-Oxley places personal responsibility on corporate management to establish and maintain an adequate internal control structure and procedures for financial reporting.

Among other things, these controls include security measures that must ensure employee Internet access is compliant with the company's established policy, without any ability to bypass it. Company executives are held personally and legally liable for failing to comply with SOX regulations, which makes the deliberate circumvention of corporate Internet use policy a critical concern for organizations.

## Threats Posed by Anonymizers

Because of their ability to introduce malicious exploits in to networks, and because they introduce legal liabilities by enabling employees to circumvent Internet or acceptable use policies, anonymizers pose the following threats to an organization:

- Allow employees and students to access inappropriate and potentially harmful sites prohibited by Internet use policy
- Expose organizations to malicious threats including drive-by spyware, viruses and Trojans
- Expose users to identity theft, pharming, and phishing attacks
- Expose users and organizations to information theft
- Provide anonymity for abusers of corporate resources
- Prevent Web filters from monitoring users' online activities

## Why Content Filtering Provides only Limited Protection

Although most Internet filtering solutions include an "Anonymous Proxy" or "Proxy Avoidance" category in their databases, they actually fail to block access to Web-based proxies due to their "list-based" approach. "List-based" products cannot keep up with the increasing number of new anonymizing sites. The fact that users can easily install anonymizing tools on their private computers makes it even more difficult.

The following quote from one of the URL filter vendors can clearly show how ineffective such solutions are: "To date, <XYZ> has added 24,000 anonymizer sites to their database in 2007; 6,000 sites were added in the third quarter as sites proliferate." Simply trying to add more and more anonymizer URLs to a database is not an adequate solution. Due to their extremely quick proliferation rate, it is essentially impossible to maintain an updated list as new anonymizer URLs are being developed by the minute.

This is demonstrated by example in the following screen shot from a real conversation on a discussion board:

**victoria wrote:**

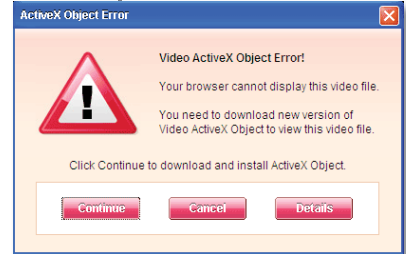
So, I'm a junior and I've been working on this "hacking" thing for a while now-- since 4th grade. I've beaten bess, some LAME firewall they used at my high school freshmen year and a dozen other proxies on my work computers. It took me about two weeks but I finally found a way to beat web. **XXX** use this:  
de.web-blaster.org  
Although you can't login to your myspace, you can view your profile by typing in the url. I'm still working on it, but it's progress.

Additionally, one of the most crucial elements making anonymizing tools a leading security threat and highly problematic for most security products is the HTTPS/SSL support offered by many of these servers. More than 30% of the Web sites that offer anonymous surfing allow HTTPS/SSL connections.

Standard URL filtering solutions are unable to adequately protect against HTTPS/SSL Web sites because the entire content, including the URL itself, is encrypted (the entire HTTP header is encrypted together with the data). The only information that a URL filtering product can see in this case is the IP address of the Web server, which effectively turns the URL filtering product into an IP address filtering solution. Filtering IP addresses is not a reliable technique since the IP can easily be changed, and on shared servers (used by many pornographic Web sites), one IP address can belong to several domains (URLs).

Another example of the limitations of URL filtering is the latest trend in malware development – infection through application add-ons. In this example a carefully crafted malware uses social engineering to lure users into installing a codec by presenting itself as being necessary to view pornographic material.

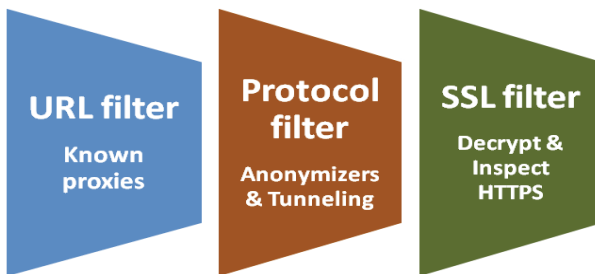
Since the actual download of the offending code is not done by the browser from a Web page but by another application (Windows Media Player in this case), there is a very small chance that this URL will ever be registered in the URL filter database.



## The eSafe Multi-Layered Solution

It has been established that blocking anonymizers requires much more than just a standard URL filter solution. The complexities and adaptability of anonymizing technologies requires a multi-layered solution that addresses not just URL filtering, but in addition provides proactive, real-time blocking based on site code and behavior, even if the anonymizers is encrypted by SSL protocols. In this section, we will discuss the multi-layer methods used by eSafe to thwart the threats of anonymizing technologies, including what makes eSafe’s Anti-Anonymizer the industry’s most unique and effective solution.

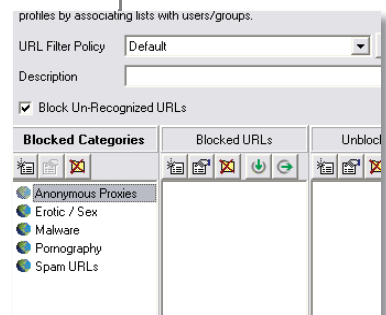
eSafe Anti-Anonymizer technology is based on three protection layers:



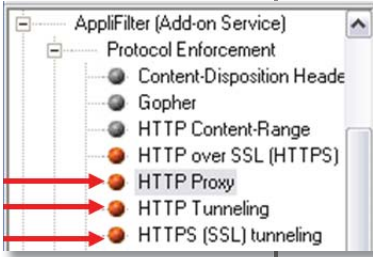
### Layer 1 – URL Filter

Similar to other solutions, the URL filter layer blocks access to all known anonymizers. eSafe uses the largest URL filter database in the world, covering 97% of all commonly browsed Web sites. This database is updated constantly throughout each day, using machine learning algorithms to classify Web sites. More than 150,000 URL entries are updated each day, more than 10 times that of other URL filtering solutions.

However, URL filters can only block what they know, and are inadequate against home-grown anonymizers running on dynamic DSL or Cable IP addresses.



## Layer 2 – Protocol Filter



This layer is unique to eSafe and no other product is able to provide such functionality. The protocol filter uses eSafe's AppliFilter™ technology to identify anonymous proxy protocols even if they are tunneled through other standard protocols like HTTP or HTTPS.

AppliFilter inspects outbound Internet traffic and can detect more than 500 signatures of different application protocols, including all anonymizer protocols and all popular tunneling applications that are used by desktop circumventors.

## Layer 3 – HTTPS/SSL Inspection



This layer provides protection against anonymizers that use the encrypted HTTPS/SSL protocol to circumvent existing security solutions. Typically when this method is used, the traffic between the client and the anonymous proxy is encrypted and thus cannot be inspected.

eSafe's Web SSL protection layer decrypts both incoming and outgoing HTTPS/SSL traffic, checks the URL, inspects the content and then encrypts it again using a certificate from a locally trusted CA (Certificate Authority).

Since eSafe Web SSL will always validate SSL certificates provided by the destination Web site, it will effectively block access to all anonymizers with self-signed, invalid, expired or revoked certificates. This by itself prevents access to the majority of home-brewed anonymizers.

## Summary

The eSafe Anti-Anonymizer feature is based on three layers of defense that include dynamic parsing and analysis of protocols used by anonymizers, even when traffic is tunneled through standard HTTP.

	eSafe	Other solutions
Block known anonymous proxies	✓	✓
Block anonymizer protocols	✓	✗
Block tunneled protocols	✓	✗
Block SSL/HTTPS anonymizers	✓	✗



For more contact information, visit: [www.Aladdin.com/contact](http://www.Aladdin.com/contact)

North America: +1-800-562-2543, +1-847-818-3800 • UK: +44-1753-622-266 • Germany: +49-89-89-4221-0 • France: +33-1-41-37-70-30 • Benelux: +31-30-688-0800 • Spain: +34-91-375-99-00  
Italy: +39-022-4126712 • Israel: +972-3-978-1111 • China: +86-21-63847800 • India: +919-82-1217402 • Japan: +81-426-607-191 • All other inquiries: +972-3-978-1111