

Anonymizers – The Latest Threat to Your Web Security

This white paper, written for executives and IT professionals, explores the growing dangers of anonymizers, an unfortunately very effective technique for circumventing Web use restrictions. The white paper also describes how the iPrism® solution from St. Bernard® combats anonymizer tactics through dynamic filtering and classification methodologies for superior Web protection from internal and external threats.

What You Don't Know Can Hurt You

"Anonymization," in general, is as simple as users covering their tracks as they browse the Internet. One of the more prolific and easy-to-use masking tools are collectively known as "Web-based proxy servers" or Web-based proxies." These Web servers, also known as anonymizers, forward client requests to other servers, but they remove identifying information from the web access requests.

Anonymizers have legitimate as well as suspicious uses. They protect IP address and related identifiers from web sites or hackers that seek to eavesdrop or surreptitiously extract information from unsuspecting Web site visitors. Anonymizer sites funded by non-profits enable citizens of countries with repressive governments to communicate on the Internet without fear of reprisal. Using an anonymizer is not illegal, but using one to conduct illegal activity without being traced is.

Covering Their Tracks: How Anonymizers Work

Anonymizer Web sites act as go-betweens. Users log onto a Web site and type in a destination, and the proxy server surfs the Web for them. The anonymizer then passes the results of the search back to their browser, often via an encrypted communications channel, to mask both the identity of the target Web site and the relayed contents.

Open-source anonymizer software kits allow people to create proxy servers on their home computers and access them from their workplace or schoolroom. These "one-off" anonymizers are extremely hard to detect because there is no Uniform Resource Locator (URL) for which an organization can search, just an innocent-appearing IP address.

The Dangers of Anonymizers

Certainly uncontrolled Web use creates a nuisance for organizations, hijacking network bandwidth for downloading large audio and video files, and encouraging time-wasters to engage in non-work-related Web surfing.

But unchecked Web use carries significant risks. In schools and libraries, anonymizers are the most popular tool students use to access top social Web destinations such as YouTube, MySpace and Facebook, typically blocked by school IT staffs. Anonymizers also circumvent blocks to potentially harmful sites prohibited by district acceptable use policies (AUP). And, as recent news articles reveal, even innocuous social Web sites can be frequented by sexual predators or serve as a launch pad for harassment. A recent Kameron Institute Research report unveiled that cyber bullying incidents range from 18 to 42 percent of students in grades 4 through 8. In addition, 21 to 49 percent of students in grades 6 through 12 say they have been bullied online.

Non-compliance with the federal Children's Internet Protection Act (CIPA), written to protect minors from obscene or pornographic content or physical or emotional harm, can result in legal liability and fines or loss of funding. State and regulatory agency laws also carry heavy penalties. In the workplace, anonymizers give employees access to offensive or illegal content by making end-runs around corporate network defenses. These isolated breaches can precipitate costly and public lawsuits if co-workers are exposed to content.

The potential damage, albeit serious, doesn't end there. Anonymizers create huge network security holes, hacker portals for data theft, spyware, viruses and worms—dangers of which users are typically completely unaware. Anonymizer sites and fringe sites that offer illegal or offensive content often covertly deliver malware applications. For example, even after the original computer user logs off, the machine can start delivering offensive popups to other users who log on to that computer.

Anonymizers a Fast-Growing Threat

To date, St. Bernard® has added 24,000 anonymizer sites to their database in 2007; 6,000 sites added in the third quarter as sites proliferate.

Your Best Protection Against Anonymizers

As a school or library administrator or employer, you are responsible for creating and maintaining a safe, comfortable, harassment-free, and discrimination-free environment. Your organization needs to define fair and consistent AUPs, educate users about the reasons for those policies, and enforce them without fail.

The first step is to create and distribute written policies that notify students and employees that Internet access is a tool for learning or business. Next, you need to educate users by describing the dangers to their co-workers and friends, as well as the liabilities to the organization, as a result of engaging in potentially risky Internet activities.

But don't believe that you can leave compliance to chance by implementing just the first two steps. Best practices dictates that you must combine written policies and user education with powerful but flexible monitoring, filtering and blocking mechanisms to drive home your organization's convictions. *(For more information on creating effective AUPs, download the iPrism ePolicy Handbook at www.stbernard.com/forms/policyhandbook/ph_ip.asp.)*

Web Protection When Firewalls Aren't Enough

All firewalls block incoming traffic, and higher quality firewalls block specific outgoing traffic according to what you specify in access control list (ACL) "rules." However, firewalls filter network traffic by IP address or network port information. This approach doesn't work well for Web filtering because many Internet service providers (ISPs) employ a content delivery system that associates many IP addresses with one URL, hosting multiple Web sites on the same server. Blocking solely by IP address incorrectly blocks every site on a hosted Web server, even though some sites may not contain inappropriate content.

To effectively block Web-based traffic, you need to block Web site URLs. However, blocking URLs involves time-consuming configurations to the Domain Name Service (DNS) server. These sites are so pervasive that many businesses lack the technical staff to keep up with the constant changes. Others may not have access to the DNS server if those organizations use the DNS services of their ISP. Organizations that hire out their network support can find the frequent changes to their firewall or DNS server needed to keep their protection up-to-date costly and inconvenient.

What's needed is an easy to use but flexible security solution that blocks Web sites and keeps up with the constantly shifting Web landscape. The solution also needs to provide drilldown visibility into what users are doing and the comprehensive reporting to respond to regulatory detailed reporting requirements and legal audits.

St. Bernard iPrism: A Plug and Play Appliance

iPrism is St. Bernard's award-winning, dedicated Internet filtering appliance that protects your organization from Web-based threats at the perimeter, before they can reach your internal servers. Its hardened, optimized operating system eliminates security flaws and troubleshooting complications associated with multiple-party server solutions. The single-vendor solution also facilitates troubleshooting since you have only one responsible party for support and service.

The iPrism appliance runs only those processes that are required for Web filtering, for focused, maximized performance. Server-based systems, in contrast, run other processes that can compromise stability, accuracy and control. iPrism's proprietary kernel-level filtering technology delivers the speed of pass-by methods with the accuracy of pass-through methods, minimizing false positives and false negatives.

iPrism was recognized for "Excellence in URL Filtering Customer Trust" in April 2007. Once a year, the editors of the Info Security Products Guide, published by Silicon Valley Communications, grant Global Excellence Awards to distinguished security products.



"iPrism turned out to be a 'fire and-forget' solution. It was extremely easy to install and requires virtually no maintenance—unlike the software-based Internet filtering solutions that we considered."

—Darrell Clay,
IT Technical Supervisor,
Lodi Memorial Hospital

Powered by the iGuard 100 percent human-reviewed database, the most accurate in the industry, iPrism provides 24/7 protection from dangers associated with instant messaging (IM), peer-to-peer (P2P) networks, spyware, malware, and phishing—as well as anonymizer sites.

iPrism is a completely self-contained solution designed for easy installation, configuration and management, and virtually zero maintenance. Automatic database and system software upgrades continually refresh your network's protection. iPrism includes comprehensive monitoring and reporting “on-box,” with no additional hardware or software required.

- 82 percent of decision makers indicated that they want to maintain control of their e-mail environment.
- 68 percent said that in-house management is more flexible than outsourcing.
- 63 percent maintained that they are concerned about the security of their data in the hands of a third party.

In addition to control and security concerns, managed service solutions for secure content management generally have weaker user directory integration than appliance solutions and can only detect the loss of data or proprietary information once it has left the organization's network.

The Most Efficient and Accurate Web Filtering on the Market: How iPrism Works

As shown in Figure 1, iPrism sits between your organization's network and the Internet, functioning as an in-line transparent bridge. All network traffic destined for the Internet passes through it before reaching your firewall. The solid, platform-independent Unix-based appliance works in virtually any environment.

Since the iPrism bridges traffic, you don't need to change the IP addresses of desktop computers or change any settings. There is also no need to install additional software or upgrade equipment. And your network users don't know the system is there until they encounter a blocked Web site notice.

The customizable “access denied” notification screen informs users of blocked access attempts and informs them that their actions are being logged. Our customers report that the screen itself can act as a powerful deterrent to future attempts.

Because of its location in the network, iPrism can filter mobile traffic, an important attribute in today's fluid business environment. Using filtering policies set by your IT support, proxied web traffic from remote or mobile users is easily and accurately monitored and blocked.

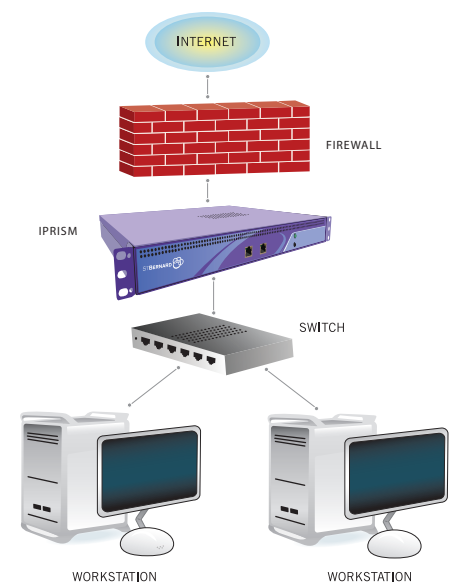


Figure 1. iPrism as an In-line Transparent Bridge

iPrism protects your organization through both reactive URL filtering and proactive pattern recognition filtering.

URL Filtering

iPrism filters Web site traffic by full URL names, a process required to properly handle virtual Web site hosting. Instant messaging and peer-to-peer applications can also be blocked using the same process, without additional subscription charges. Kernel-level URL filtering rapidly transfers data between input and output drivers, bypassing slow kernel-to-user data level transfers and content switching. *(For more detailed information, read [The Powerful Technologies Behind Best-of-Breed Internet Filtering](#), found on the St. Bernard iPrism Resource Center, www.stbernard.com/products/resource/center_ip.asp.)*

The iPrism iGuard database contains over 80 Web sites categories and millions of URLs. To create a profile for specific group or user, you simply create a profile name and identify the iGuard categories to monitor or block. iPrism's flexible ACL technology allows specific categories such as shopping, banking and online auctions to be accessible during special times of the day, such as lunch, but not accessible during work hours. Managers or others with override privileges can enter a password to immediately access and examine blocked Web sites.

“**Being able to set up different filtering rules according to a group's or individual's needs has increased my team's efficiency, saved labor costs and reduced user frustration.**”

—Joe Huber,
Director of Information Systems,
Greenwood School District

iPrism is the only Internet filtering solution on the market today that uses a 100 percent human-reviewed database. Human-powered intelligence produces the highest level of filtering accuracy, with the lowest levels of false positives and false negatives—far superior to strict content analysis heuristics or blended classification solutions. The iGuard team actively researches and adds new anonymizer Web sites to the database, protecting your organization from new threats by automatically sending updates to your database every day. The critical Security category covering spyware, malware and phishing is updated hourly.

Zero-Day Packet Pattern Filtering

In addition to human review, iPrism adds another layer of filtering to defend against anonymizers. To address single-user proxies, artificial intelligence agents in the iPrism operating system analyze patterns in the request URL. When the data forensics detects a suspicious pattern in the URL, it dynamically blocks access to the site. The iGuard team also actively identifies unique and consistent patterns to assist in dynamic real-time classification. iGuard's current pattern list provides excellent coverage for proxy packages such as PHPProxy and CGIProxy. Pattern updates are published in the critical hourly filter updates to all iPrism customers.

iPrism allows a user to surf a proxy Web site (if it's not in iGuard), but once he or she attempts to use the site to perform a request of the target Web site, the patterns are detected and blocked.

Together, the iPrism filtering mechanisms help you:

- Avoid overblocking users, so that their productivity isn't compromised and you aren't inundated with help requests
- Avoid underblocking users, so that your Internet access returns to being more of an asset than a liability
- Choose an Internet filtering solution with a classification system aimed at accuracy first and foremost

Comprehensive Activity Monitoring and Reporting

Monitoring and reporting is another area where iPrism earns its justifiable reputation. Don't let the simple interface fool you, iPrism's powerful Report Wizard can supply a complete profile of user activity to meet your exact requirements, quickly and easily. As shown in Figure 2, you can start with an overview of usage, by time, bandwidth or URL requests, then quickly drill down to a detailed view of each user. You can also turn on real-time monitoring for an immediate look at your Web traffic to help you better manage network bandwidth usage.

Comprehensive monitoring tools help you spot trends or behaviors that may need to be addressed in your acceptable use policy. They also help you identify potential trouble spots so you can take action. Once more, the reports provide incontrovertible evidence of a user's inappropriate browsing that can be used to take corrective action with a student or employee, or in the worst case, substantiate lawful expulsion or termination.

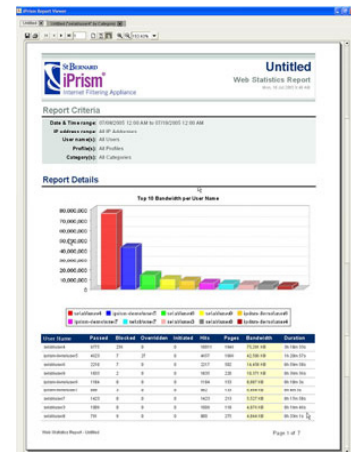


Figure 2. iPrism Report Wizard Detailed Report

You can Trust St Bernard

St. Bernard Software, Inc. (OTCBB: SBSW) is a global provider of security appliances and hosted solutions, including secure content management and archiving. The company's award-winning products deliver innovative security solutions that offer the best combination of ease-of-use, performance and value.

Established in 1995 with headquarters in San Diego, California, and international offices in the United Kingdom, Australia and the Netherlands, St. Bernard sells and supports its products directly and through solution partners worldwide. For more information, please visit www.stbernard.com.