

Providing Safe Web Access in Educational Institutions

RELEASE 3
DECEMBER 2011

Educational institutions today provide widely available Internet access to enhance the learning experience. When used appropriately, the Web is an invaluable academic resource and a channel to deliver customized content. However, with technologies like Web 2.0 being heavily focused on the social aspect of the Web, the Internet is also used for the rapid and widespread proliferation of inappropriate or even malicious content. Consequently, educational institutions have to balance the sometimes conflicting requirements of providing access to the best available educational resources while ensuring Internet safety by protecting against harmful content and implementing internal policies.

Challenges

- **Malware:** Long gone are the days that computer viruses were experiments conducted by individuals with no specific aim. Web criminals today continuously develop new methods to compromise computers connected to the Internet. In addition to regular spyware and virus attacks, more creative exploits include botnets to host and deliver malicious software, keyloggers to steal passwords, phishing to monitor users' Web browsing habits or Trojans for surreptitious access to computers.

Computer users can trigger these attacks not only via file downloads, but also through casual browsing to seemingly secure Web sites. Compromised Web sites can exploit security weaknesses in the browser or deceive the user to initiate the installation of malicious software as "drive-by" installations. This threat vector is even more relevant in the context of a user base, for example students tend to have unpredictable browsing habits. In fact, Barracuda Networks' studies indicate that students are more likely to visit compromised Web sites than any other group of users.

- **Criminal Activity:** The anonymity and social reach afforded by the Web has made it a vehicle for sexual predators and other such criminals to victimize youngsters. Children can inadvertently identify themselves to such elements through chat rooms, instant messaging (IM), social networking sites or other avenues, thereby making them vulnerable to cyber-bullying or online stalking tactics. This form of cybercrime is a very unpleasant reality today and is a major concern for parents and administrators.
- **Instant Messaging (IM)/Peer-To-Peer (P2P):** Peer-to-Peer file transfer systems such as BitTorrent and KaZaa and IM applications like AOL Instant Messenger, ICQ and Google Talk, enable users to communicate in real-time and directly transfer files between client computer systems over the Internet. In addition to the obvious productivity impact, this exposes a significant security risk since files shared online may be "poisoned" or otherwise misrepresented to entice users into downloading them. File transfers can also consume a large amount of bandwidth, degrading network performance and undermining legitimate purposes for which Internet access is provided. Furthermore, P2P mechanisms are commonly used to illegally download protected content like copyrighted music, movies or software. International copyright regimes and copyright law hold institutions legally liable for the actions of their users. Laws such as the Copyright Designs and Patents Act (1988 – UK) and the Digital Millennium Copyright Act (1998 – US) encompass all intellectual property, print or digital. Regulating IM/P2P technologies is therefore a necessity for educational institutions.
- **Regulatory Compliance:** Educational Institutions are often subject to regulatory compliance requirements like the Children's Internet Protection Act (CIPA). Enacted in 1998, CIPA imposes requirements on schools and libraries in the US that receive funding for Internet access. Broadly speaking, schools and libraries are required to demonstrate that they are equipped to monitor the online activities of minors, restrict access to pornography and other objectionable material, and prevent unauthorized access and other illegal activities such as hacking. Also certain organizations, such as UK's Internet Watch Foundation (IWF), serve as a repository for potentially illegal online content and partner with the industry, government and law enforcement to minimize the proliferation of such content.
- **Anonymous Proxies:** As students become more technically savvy, they inevitably seek ways to circumvent restrictions to online content. Anonymous proxies aid this by providing Web sites or applications that are designed to avoid Web filtering policies by obfuscating user identity. Widespread use of these applications will expose an educational institution to all the risks inherent to an unfiltered, unmanaged IT infrastructure.

- **Access Levels:** Any educational institution has constituents that require different levels of Web access. For example, faculty and staff could need access to content that is not appropriate for students, secondary school students could be provided access to content that should not be available to primary school children and so on. There are very few academic environments where a uniform Web access policy will satisfy the requirements of all users.
- **Forensics:** School administrators are often required to resolve disputes or to address concerns or complaints from parents or regulators over Web access. Accurate and comprehensive forensic data will help educational institutions make informed decisions in these sensitive situations.

Barracuda Web Security Solutions

Barracuda Networks Web filtering solutions help educational institutions provide safe and regulated Web access while protecting against the latest emerging malware threats and enabling regulatory compliance. Available as the Barracuda Web Filter appliance or as the Barracuda Web Security *Flex*, these solutions are designed to protect against Internet threats and enforce acceptable Internet usage policies. They combine preventative, reactive and proactive measures to form a complete content filtering and anti-malware solution.

The capabilities include:

Anti-Malware

Barracuda Networks appliance and service based solutions include a range of award-winning spyware and virus protection capabilities including blocking access to known malicious Web sites and blocking virus and spyware downloads. Through multiple layers of anti-malware technology, they can protect against sophisticated attacks like drive-by downloads and even secure the network by detecting any existing Spyware applications and blocking their access to the Internet.

The Barracuda Web Filter and Barracuda Web Security *Flex* are backed by Barracuda Labs, a 24x7 advanced security research center that analyzes data from emails, URLs and other information from tens of thousands of collection points worldwide and also from contributions from more than 100,000 Barracuda Networks customers. As new threats are identified, the latest malware definitions and defense mechanisms are automatically activated, ensuring the network is guarded effectively.

Content Filtering

Administrators can regulate access to Web domains classified across multiple categories. These include categories of particular interest to educational institutions such as adult, pornography, violence, criminal activity, alcohol and tobacco, as well as spyware sites and anonymous proxies. Network administrators can choose to block, accept, warn or monitor access to these domains based on institution policies. The solutions can also leverage "safe search" filtering capabilities built into image search engines and automatically rewrite URLs for image searches to restrict objectionable content.

The Barracuda Networks content categorization process employs several mechanisms including extensive human review, automatic crawlers, and public and proprietary directories. Barracuda Networks also partners with organizations like the Internet Watch Foundation (IWF) to keep up to date with the latest lists of potentially unsafe Web domains.

Barracuda Networks solutions are ideal for educational institutions concerned with enforcing safety and regulatory compliance, like CIPA, in an easy and cost-effective manner.

Safe Access to Educational Videos

Barracuda Web Security solutions provide students with safe access to educational videos by seamlessly integrating with the YouTube for Schools portal for educational video. When enabled, any requests to YouTube will be automatically redirected to the YouTube for Schools portal. This is particularly useful for IT administrators in educational institutions to provide safe and regulated access to the wealth of educational content on YouTube while restricting access to objectionable content.

Application Blocking

In addition to Web sites, administrators can regulate usage of Internet applications such as IM clients, Internet music applications, software updaters, Skype, popular browser toolbars, P2P applications and proxies. This prevents students from abusing bandwidth and Internet resources, sharing unsafe files and compromising school computers with viruses or malware. Institutions can thereby minimize

security risks, maximize the utility of their information systems, and reduce the threat of legal liability for copyright infringement or other compliance frameworks. Unlike alternative solutions that rely on third-party auditing tools, the Barracuda NG Firewall has integrated its Revision Control System (RCS) directly into the security architecture so that the audit control cannot be circumvented either intentionally or unintentionally. The advantage lies in the absolute reliability and completeness of the recorded configurations changes, offering major benefits both for resolving faults and also providing evidence.

Policy Management

Both the appliance and service-based solutions include a powerful policy engine that supports granular policies by user, group, IP address ranges or time. Separate policies can be applied to domain users (authenticated) and guests (unauthenticated). In addition to built-in content and application categories, they also allow for creation of allow lists ("whitelists") and block lists ("blacklists") to control access to specific domains. Administrators can specify URL patterns using the UNIX regular expression (regex) syntax and restrict downloading files from the Internet based on MIME types, such as executables, streaming media or videos. In addition, time-based exception rules can be created to override global policies. Using these powerful tools, educational institutions can design Internet controls to precisely match the requirements of students, faculty and staff while enforcing safe use policies and complying with regulations.

Reporting

The Barracuda Web Filter and Barracuda Web Security *Flex* enable extensive forensic analysis by way of detailed logs and reports on Internet activity. Reports can be generated on users' Web browsing activity, by domains and content categories, by time spent online, or by their bandwidth consumption. Reports can be scheduled for automatic delivery as well. For example, a school district can schedule reports to be sent out to principals detailing Internet activity at each school site. Such information can be used by administrators to monitor Internet activity, budget network resources and prevent online misconduct.

The Barracuda Web Filter and Barracuda Web Security *Flex* provide the Barracuda Web Security Agent (WSA), a downloadable client that be installed on remote, off-network computers. With the WSA installed, Web traffic from remote client computers will be transparently filtered either through a central Barracuda Web Filter appliance or through the cloud based service, ensuring that Web browsing policies applied to users within the network are also enforced for off-network users. The Barracuda WSA can be centrally configured and deployed and is tamper-proof once installed on client computers. This enables organizations to implement a consistent Web security policy across localized and distributed workforces without the need to invest in or manage additional solutions.

With a combination of powerful features, ease-of-use and affordability, the Barracuda Web Filter appliance and Barracuda Web Security *Flex* provide flexible deployment options for educational institutions to secure their networks and provide a safe and productive Web access environment.

For questions about the Barracuda Web Filter, please visit <http://www.barracuda.com/webfilter> or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit <http://www.barracuda.com/products>.

About Barracuda Networks Inc.

Barracuda Networks Inc. combines premises-based gateways and software, virtual appliances, cloud services, and sophisticated remote support to deliver comprehensive content security, data protection and application delivery solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 150,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif.



Barracuda Networks

3175 S. Winchester Boulevard
Campbell, CA 95008

United States

+1 408.342.5400

www.barracuda.com

info@barracuda.com