Social Media Control with the Barracuda Web Filter

Securing the power of the collaborative Internet through discovery, policy control and archiving for compliance

RELEASE 1
JULY 2012

While Social Media and applications enable rich user interaction and collaboration, they also open the door to a variety of threats like social media scams, identity theft, Trojans, phishing attacks, botnets, advanced persistent threats, cyber-bullying and data leakage. During the early years of social media, most organizations blocked access to these sites in the workplace because their adverse impact on productivity. However, today's IT administrators have the dual challenge of providing access to selected Web 2.0 resources while ensuring the security of the network and the safety of users. This is particularly challenging because of the mashed content on social media portals. For example, an organization may want to use Facebook or Twitter for viral marketing campaigns but prevent employees from playing games on Facebook or leaking confidential company information through Twitter. This is difficult with traditional content filtering solutions since they either completely block or allow unrestricted access to this type of content and applications.

The Barracuda Web Filter provides extremely granular control over Web 2.0 sites and applications. Administrators can also configure the Barracuda Web Filter to archive outbound social media communications, like Facebook posts, tweets and web-based email to a message archival solution, like the Barracuda Message Archiver. These messages can be indexed and then mined for forensic analysis.

Sample use-cases

- Improve productivity by blocking access to Facebook games or Facebook chat while allowing access to Facebook.
- Restrict access to the "Jobs" section of business networks like LinkedIn to selected groups within the organization.
- Provide safe access to educational videos on YouTube.
- Avoid data leaks, prevent cyber-bullying, enforce compliance and improve auditability by monitoring outbound social media communications for sensitive content and creating forensic reports.
- Prevent data-leaks and malware infections by inspecting SSL transactions to untrusted web sites while maintaining confidentiality of trusted transactions.

Key Features

Granular Web 2.0 Application Control

From its inception, the Barracuda Web Filter combined basic policy controls with layer 7 protocol analysis to regulate a variety of bandwidth intensive applications. This includes public IM clients, streaming media applications, Skype, P2P file sharing applications like BitTorrent and several others. This allows administrators to optimize bandwidth usage by only allowing mission critical applications in the workplace.

In addition to this, the Barracuda Web Filter also provides the ability to regulate the usage of social media and other web based applications. This includes applications and actions available through sites such as Facebook, LinkedIn and Twitter. For example, an administrator can allow access to Facebook but block Facebook email, Facebook chat, Facebook games or prevent data leaks by blocking Facebook comments. This level of granularity allows organizations to provide mission critical access to Web 2.0 sites while restricting non-productive actions and applications.

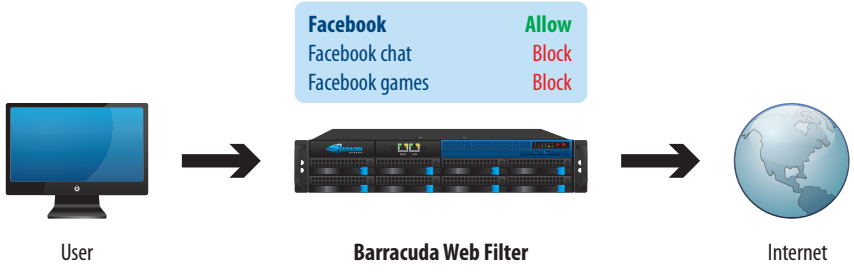

Fig 1. Web Application Control

Better Visibility with Web Application Monitoring

Gone are the days when corporate email was the primary communication channel for corporate networks. Today users can post messages on Facebook, send tweets or use LinkedIn email for this. As organizations try to embrace social media in creative and engaging ways, they also need to ensure the security of these new channels. This is particularly relevant to financial institutions and educational institutions where social media abuse can lead to liability issues or encourage undesirable activities like cyber-bullying.

The Barracuda Web Filter provides a unique set of turn-key capabilities to monitor social media communications from portals such as Facebook, LinkedIn and Twitter. The Barracuda Web Filter can inspect and catalog outbound content and forward to an external message archiver, like the Barracuda Message Archiver. These messages can be tied to the users Active Directory credentials and fully indexed making them as easy to search as Exchange emails. This ensures that social media communications from corporate networks are always available for access and retrieval for eDiscovery and audits as well as to create alerts for proactive monitoring.

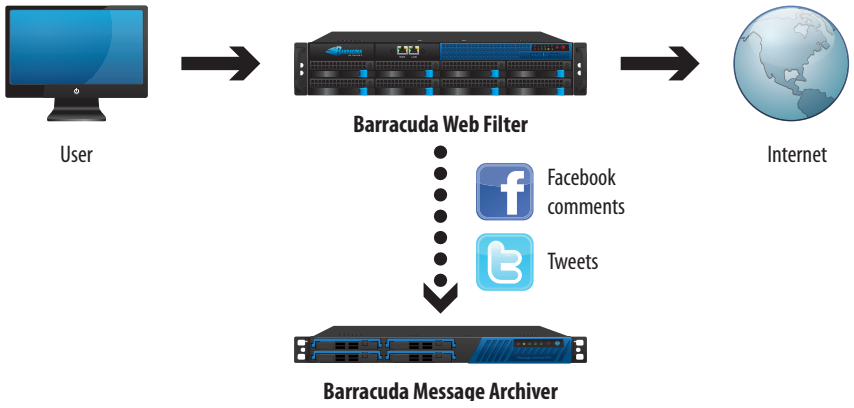

Fig 2. Web Application Monitoring

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.

Advanced Protection through SSL Inspection

SSL-encryption allows web servers to securely authenticate and exchange information with clients. As a result, the volume of SSL-encrypted traffic has grown (over ⅓ of enterprise bandwidth by some estimates) with the increasing adoption of cloud computing for enterprise applications. Also, many Social Networking sites use HTTPS for security.

This is a double-edged sword. While SSL-encryption ensures that your online banking transactions are confidential, it also makes it difficult to inspect the traffic from a security perspective. While traditional web content security systems are good at inspecting HTTP traffic, HTTPS transactions can be used to bypass company Internet usage policies or sometimes act as a channel to spread malware. For example, a user could leak sensitive content over HTTPS transactions on Facebook.

The Barracuda Web Filter provides the ability to filter as well as inspect SSL-encrypted traffic. While basic URL filtering policies will apply to all HTTPS requests, administrators can specify domains and URL categories for which SSL-encrypted traffic will be decrypted, scanned for policy and malware and then re-encrypted to the destination when deemed safe. This selective SSL inspection ensures the integrity of confidential transactions like those to banking sites while scanning HTTPS content that might be malicious.

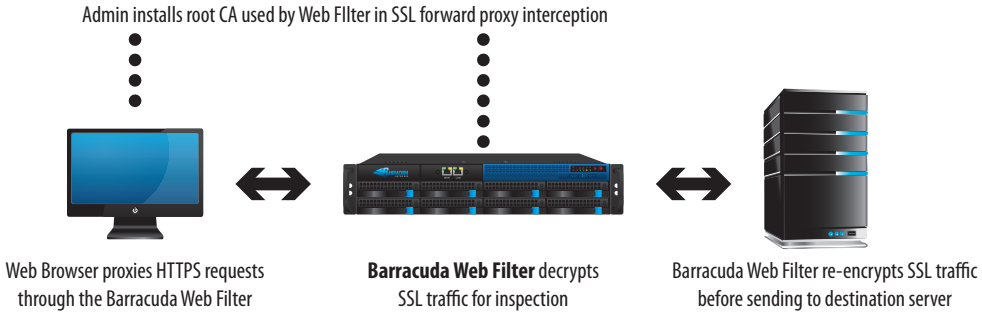

Fig 3. SSL Inspection

As shown in Fig 3. Administrators can install a root certificate on the Barracuda Web Filter that will be used to intercept, proxy and inspect the HTTPS Session.

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. For more information, please visit www.barracudanetworks.com

Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
+1.888.268.4772
www.barracuda.com
info@barracuda.com