Social Media Control with the Barracuda Web Security Gateway

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

White Paper

While social media and Web 2.0 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, cyberbullying, and data leakage. During the early years of social media, most organizations blocked access to these sites in the workplace because of 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 network security and user safety. This is particularly difficult 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 information through Twitter. This is problematic with traditional content filtering solutions since they either completely block or allow unrestricted access to these types of content and applications.

The Barracuda Web Security Gateway provides extremely granular control over Web 2.0 sites and applications. Administrators can also configure the Barracuda Web Security Gateway to archive outbound social media communications, like Facebook posts, tweets, and web-based email to a message archiving solution, such as 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 other Facebook features.
- 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 cyberbullying, 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 websites while maintaining confidentiality.

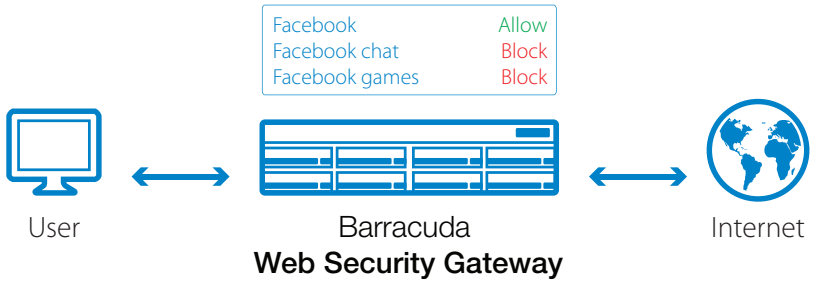
Key Features

Granular Web 2.0 Application Control

From its inception, the Barracuda Web Security Gateway 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, the Barracuda Web Security Gateway provides the ability to regulate the use 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, and 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 and educational institutions where social media abuse can lead to liability issues or encourage undesirable activities such as cyberbullying.

The Barracuda Web Security Gateway provides a unique set of turnkey capabilities to monitor social media communications from portals such as Facebook, LinkedIn, and Twitter. The Barracuda Web Security Gateway can inspect and catalog outbound content and forward it to an external message archiver, such as the Barracuda Message Archiver. These messages can be tied to the user's Active Directory credentials and fully indexed, making them as easy to search as Exchange email messages. This ensures that social media communications from corporate networks are always available for access and retrieval for eDiscovery and audits. It also allows the creation of alerts for proactive monitoring.

Fig 2. Web Application Monitoring

Proactive Alerts for Suspicious Activities

As an extension to web application monitoring, the Barracuda Web Security Gateway includes pre-built English-language dictionaries of keywords and phrases pertaining to harassment, weapons, terrorism, or pornography. Administrators can configure the device to automatically generate alerts when content containing these keywords or phrases is posted to social media portals or search engines. Administrators can also add their own keywords and phrases for monitoring. The alerts are tagged with real network user identities, making it easy to identify the source, independent of online profiles.

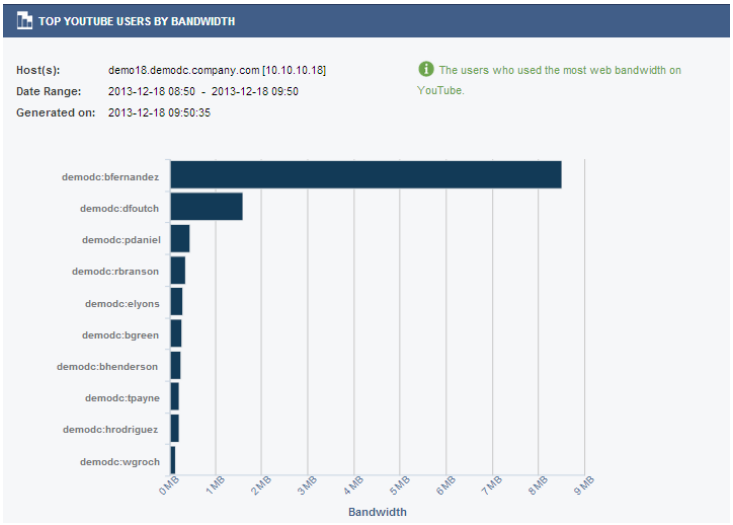


Fig 3. Report of Top YouTube Users

Safe Access to Educational Videos

Barracuda Web Security solutions provide students with safe access to educational videos by seamlessly integrating with YouTube Safe Search for educational videos. When enabled, any requests to YouTube will be automatically filtered with YouTube Safe Search results. This makes it easy 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 (more than one third of enterprise bandwidth by some estimates) with the increasing adoption of cloud computing for enterprise applications. Also, many social networking sites and search engines 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 Security Gateway 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, 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.

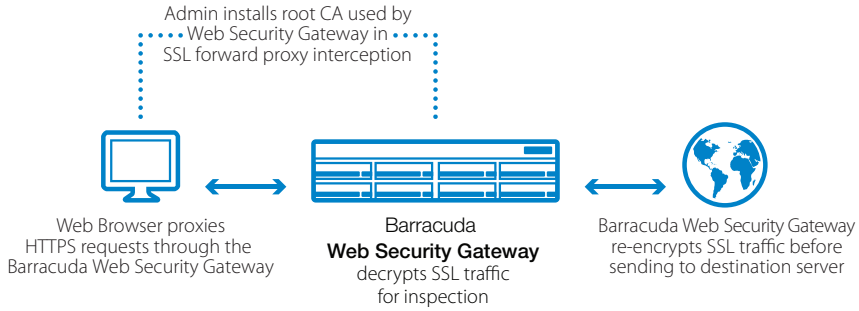


Fig 4. SSL Inspection

As shown in Fig 4. Administrators can install a root certificate on the Barracuda Web Security Gateway that will be used to intercept, proxy, and inspect the HTTPS Session.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.