Threat Containment for Facebook

Based on statistics for more than 62M users in 2009, the Blue Coat WebPulse™ cloud service ranked social networking as the number one most requested web category, surpassing web advertisements, search engines and even webmail. This represents over 25% of all web requests in the top 10 most requested web categories. However, taking this number one position has come with a price. Facebook also claimed top status as one of the most targeted phishing sites, along with being subjected to additional threats like the Koobface worm. This technical brief discusses multiple Blue Coat solutions to address malicious content control, enforce acceptable use policies, prevent sensitive information leakage and enhance user productivity on Facebook.

Introduction: A Hybrid Approach

Blue Coat utilizes a layered defense to stop web threats. The first layer uses Blue Coat WebFilter, a content filtering solution that offers over 80 categories, supports over 50 languages, has more than 70 million worldwide users and provides more than seven billion web ratings per day. WebFilter utilizes the WebPulse cloud-based community defense that analyzes over 2B real-time input user requests per week to detect the latest web threats and rate the latest web content. WebFilter provides up to four ratings per web request. For example, facebook.com/games/drinkingwars is rated as Social Networking, Games, and Alcohol. Overall, WebFilter has more than 40 categories just inside of Facebook, providing a nested view of user activity that single flat rating URL schemes cannot provide.

Dynamic URLs in Facebook are a leading threat vector, as we have all seen prompts about photos and videos with links to view them. “Is this a picture of you?” is a link often sent to friends from a compromised user account. One click leads to a video codec or software update installing malware on the friend’s system only to repeat the cycle to their circle of friends. WebPulse follows dynamic link chains and utilizes over 16 different threat detection technologies to detect malware downloads and block them for Facebook users. Full visibility into web threats, content and traffic patterns are provided by Blue Coat Reporter 9 with dashboards and drill-down analysis, plus 50+ pre-defined, easily customizable reports.

The second layer of defense is inline anti-malware detection, which provides protection for areas where additional visibility is required, such as SSL traffic and user authenticated or tokenized web traffic. Using Blue Coat ProxyAV™ for inline anti-malware detection with behavioral analysis on HTTP, HTTPS and FTP traffic provides threat detection for items such as webmail attachments and software downloads. ProxyAV can analyze files up to 2GB in size and up to 99 layers of compression, often larger and deeper than desktop AV defaults. Plus, using a diversity of defenses with a different anti-malware engine at the web gateway than the desktops provides additional protection. More and more web traffic is moving into SSL-protected tunnels as a default for webmail and a new option for search engines to protect privacy.

The third layer of defense is Blue Coat ProxySG with web content controls and policy to control web-based applications and protocol methods. This helps impede the use of applications such as IM, P2P, Active Content (Java), or even executable content downloads for suspicious and unrated websites. It also offers the ability to control website posts, use websites in read-only mode and disable specific web application features. ProxySG supports up to four URL filtering lists, thus allowing custom allow/block URL lists with role-based administration provided by Director to various business units, departments or regions. Examples of granular policies for Facebook using specific ProxySG controls are provided below.

The fourth layer of defense provides integration for data loss prevention (DLP) to control sensitive data leakage at the web gateway. Blue Coat DLP offers a complete solution for web, email, network and discovery that removes the complexity associated with first generation DLP solutions. Plus, Blue Coat partners with leading
DLP vendors with a certified integration partner program. The Blue Coat solution provides both data content controls, for example limiting outbound posts to web sites (making them read only), and full DLP solution integration to prevent distribution of sensitive content.

And finally, the fifth layer of defense, Blue Coat ProxyClient™, protects remote users in any location and automatically turns off when behind a ProxySG web gateway. The WebPulse cloud-based community defense provides an enhanced layer of protection over existing laptop defenses. Remote users benefit from centralized URL filtering and reporting for compliance, plus real-time web ratings and threat protection from WebPulse cloud services and defenses. Remote users are now part of a 70 million-plus user community for web awareness with 16-plus cloud defenses not technically possible on their laptop. So Facebook use at the airport, hotel or conference is filtered, reported upon and dynamic URL threats are blocked, keeping the laptop clean for its return to the organizational network.

The Blue Coat Security Solution

The Blue Coat arsenal consists of the following components: Blue Coat ProxySG, Blue Coat ProxyAV, Blue Coat WebFilter, the Blue Coat WebPulse cloud-based community defense, Blue Coat ProxyClient and Blue Coat DLP.

The ProxySG appliance enables flexible policy controls over content, users, applications and protocols. The ProxySG is a secure web gateway to enforce and control web-based traffic including HTTP, HTTPS, FTP, streaming media, P2P, IM and DNS. ProxySG was the first web gateway to offer a trusted PKI model to open and inspect SSL traffic and apply granular rules against the unencrypted traffic.

ProxyAV appliances provide inline threat protection and malware analysis of Web content at the web gateway. ProxyAV provides a high-performance architecture combined with leading anti-malware engines that efficiently analyzes Web traffic with a “scan once and serve many” caching architecture. ProxyAV has the performance ability to analyze all web content downloads – meaning no trade-offs are required, which is common with selective scanning policies in other solutions.

WebFilter is a content filtering database that runs on the ProxySG. It is the next generation of web filtering, created by combining URL filtering and web threat detection technologies together into cloud-based community defense architecture. The WebFilter URL database contains millions of website ratings, which represent billions of Web pages, cover more than 50 languages and are organized into 80 useful categories. As a result, WebFilter can provide up to four ratings per request.

WebPulse provides cloud intelligence to ProxySG web gateways, ProxyClient and K9 Web Protection remote clients. WebPulse has eight operation centers to support cloud defense analysis of over 2 billion web requests per week. New web content or dynamic links detected by WebFilter or remote clients are sent in real time to the WebPulse cloud for Dynamic Link Analysis (DLA) inspection where updates are performed. Together with the master WebFilter cloud hosted database, WebPulse provides immediate protection to web gateways and remote clients.

DLP is a content inspection appliance that allows organizations to monitor and control sensitive data transmitted in web, email, and network applications, plus discovery on information stores. Supporting multi-byte data allows for full recognition of international languages in over 600 file types with full or partial matches. Structured and unstructured data can be monitored in addition to a wide variety of information stores. Appliance-ready and policy-ready, the Blue Coat DLP solution avoids the complexity of first-generation DLP solutions.
Blue Coat Solution: Layered Security

Solution 1 – Prevent Inbound Threats via Malware, Spyware, Worms and Viruses

The most significant Facebook attack to date has been Koobface, which appeared in 2009. The Koobface worm spreads through a legitimate user’s account profile to their friends. A fake dynamic link normally associated with a picture or video (“You look funny dancing”) lures the friend to click the link, which then loads malware to the victim’s machine and continues spreading to friends in the new victim’s network.

However, it is much easier to prevent these threats than to simply block social networking sites altogether. To help agencies and organizations provide safe access to these sites, Blue Coat applies several layers of web gateway defenses to block inbound web threats from Facebook and other social networking domains. The first combines ProxySG with WebFilter, which uses threat intelligence from WebPulse to block dynamic URLs as noted above for Koobface. The second is ProxyAV inline threat analysis for malware using leading anti-malware engines and behavioral analysis.

In the first defense layer, WebPulse leverages the real-time ratings from 70 million users and 16 cloud-based defenses to quickly analyze the dynamic link chain, payloads, reputations, languages and categories. WebPulse also has over 300 automated language-categories for real-time ratings of web content, including phishing attacks. The cloud defenses analyze dynamic links, web content, active scripts and payloads for threat protection with more automation than other solutions.

Social networking users are therefore protected by the WebPulse community and cloud-hosted defenses for any dynamic link-based attacks. All it takes is one user in the community to receive a new dynamic link and report it to protect the entire community. As a result, many web threats hidden in social networking sites can be stopped before they reach the end user.

In addition, ProxySG is configured to send all respond-mod data to the ProxyAV for malware analysis, thus analyzing all web content downloads with no exceptions. Once detected, threats are blocked at the web gateway. ProxySG also applies True File Type (TFT) checks for masquerading files, and ProxyAV provides TFTs for files compressed into archives.

ProxyAV performs signature-based spyware, malware and virus scanning as well as heuristic pattern matching against all or selected content, so zero-day threats are increasingly mitigated. In the example found in Figure 1, response-mod (web responses) traffic returning from an infected Facebook account is analyzed and blocked before it reaches the user. Example:

![Figure 1](image-url)
Solution 2 – Prevent Data Leaks on Facebook

One of the key capabilities of Facebook is the ability to comment on one’s “wall.” Using Blue Coat DLP or any of Blue Coat’s certified DLP technology partners, you can configure request-mods (web requests) to be intercepted by ProxySG and sent to the DLP device for data loss analysis. ProxySG then analyzes the request against policies using data fingerprints, patterns and other variables found in documents or html data.

Once the requested data is sent to ProxySG, the outbound request-mod is redirected to the DLP. If a match is made, the DLP generates a response to ProxySG, which then sends an exception page indicating that the data is blocked, which prevents that data from leaving that web gateway. Example:

![Diagram of data flow from enterprise network to Facebook through ProxySG and DLP]

ProxySG also provides protocol method controls that can block posts used in chat and other functions with Facebook web applications. ProxySG web content controls can also restrict file uploads and file types by user or group. Together the ProxySG and DLP appliances provide a complete data loss protection solution.
Solution 3 – Block Posting of Status and Comments to Facebook

The ability to post comments on a friend’s wall can result in unintended consequences: the loss of confidential business or personal information. While Solution 2 focuses on words or phrases in HTML data or documents, Solution 3 stops users from posting information on the Facebook web application page.

Facebook uses Java and Ajax calls. Ajax gives Facebook the ability to retrieve data from Facebook servers in the background of their browser without interfering with the display of the page. Because of this, many of the controls are enforced by looking at the URI in the Ajax calls. Once there is a match of a rule in the ProxySG policy, the action associated with the rule is performed. In the case of Solution 3, the request to update status is denied to the user with ProxySG. In the policy manager, an administrator would enter the destination request URL in a regular expression: `/ajax/updatestatus.php`, with an Action of **Deny** for that URI. This rule can also be applied to requests that only query the Facebook domain. Example:

![Figure 3](image)

Any attempt to share information on the Facebook status section is also denied, and Facebook indicates this to the user. The attempt is then logged in ProxySG. Example:

![Figure 4](image)
Solution 4 – Block Games and Other Time-wasting Applications

There are thousands of games available through Facebook. These games provide several ways to lose hours of productivity. They also provide potential avenues for malicious attacks. The main Facebook page allows you to add an application through a search function or send a game as a gift to a friend.

Most applications are downloaded from http://apps.facebook.com. The URL format is typically http://apps.facebook.com/<application name>. After the user selects “Allow Application,” the application is authorized to pull your profile information, photos, and your friends’ information. The game or application then opens up in the Facebook web page, but in the background there is web data from the source game or application site that is not visible to the user.

In Solution 4, we can block all games or block Facebook applications. If the network administrator does allow games and applications on their network, it is recommended to use a minimum of ProxySG, ProxyAV and WebFilter. ProxySG and WebFilter are configured to control access to applications, as well as dynamic links leading to malware downloads. ProxyAV analyzes web response traffic for malicious inline content.

Blocking and controlling games is accomplished by using our Visual Policy Manager on the ProxySG appliance. From the GUI, go to Policy>VPM>Web Access Layer, and under the destination field, add a Request URL Category, select Games. Set the Action of Deny. Example:

![Figure 5](image)

By enforcing this policy, games are blocked with a standard or custom exception page. Example:

![Figure 6](image)
This policy rule can be qualified with the category Social Networking so only games in Social Networking are blocked, or fully qualified by using the facebook.com domain to just block games in Facebook. WebFilter provides up to four ratings per web request, which is especially helpful with blocking social networking games. Many have quite a few have triple ratings, such as alcohol, weapons, adult content and more.

In the next example, we illustrate how to set policy to block and control application downloads. This is achieved by denying access to the apps.facebook.com URL. We implement this by going into the GUI>Policy> Visual Policy Manager, and open the VPM Web Access Layer. Under the destination field, add a Request URL regular expression, and enter *apps.facebook.com*, with an Action of Deny. Example:

![Image showing GUI for blocking apps.facebook.com](image)

The same response will come back to the user when an attempt is made to access the download of an application (see Figure 6).
Solution 5 – Prevent Facebook Chat Conversations

Chat is the feature of Facebook that allows users to converse in real time with other Facebook friends. Chatting can be a huge waste of user productivity, but it also allows users to leak potentially sensitive information to other Facebook friends. ProxySG and WebFilter can help control or block chatting in two ways. The first is the ability to block All chat communications (even beyond Facebook if desired). The second is to block chat content from leaving the Facebook client. To block all Chat applications, open the GUI>Policy>VPM, Web Access Layer, and enter under Destination, Request URL Category, and select category of Chat and with an Action of Deny. Example:

Once the user logs into Facebook, the chat channel never completes and the list of friends on Facebook cannot load. Example:
This filter can be further customized to chat and social networking, or to the entire facebook.com domain because ProxySG provides a flexible policy language to AND, OR and NOR Boolean expressions.

Blocking Facebook chat transmissions is easy. From the GUI>Policy>Visual Policy Manager>Web Access Layer, and in the rule, under Destination, add a Request URL, with the Regular Expression match of: /ajax/chat, and add an Action of Deny. This regex for the URI /ajax/chat, covers chat function calls for /ajax/chat/history.php?, /ajax/chat/settings.php?, and /ajax/chat/send.php?. Example:

![Figure 10](image1.png)

This feature gives the appearance that a user can actually send chat messages to their friends. They see their friends online, but the chat transmission is blocked at the ProxySG, so whatever the user types is never received by their friend. Although this may cause user frustration and escalate Help Desk calls, the example shows the power of ProxySG. As a policy, users should receive appropriate warnings and exception alerts. Example:

![Figure 11](image2.png)
Solution 6 – Prevent Facebook Messaging (Email)

Facebook uses an application to send messages from one user to another, similar to email. In order to block messaging, at a minimum, you would need the ProxySG appliance. A rule is created in the Visual Policy Manager, under a Web Access layer, in the destination field, where you would add a request URL object with the regular expression to match /ajax/gigaboxx. The action of that rule would be set for Deny. Example:

![Image of Visual Policy Manager interface](image1)

*Figure 12*

The end result for the user attempting to send a message is a Facebook exception indicating that there is a problem. Example:

![Image of Facebook message exception](image2)

*Figure 13*
Solution 7 – Prevent Facebook Profile Update

Solution 7 prevents Facebook users from updating their profile information. This is the section of Facebook that lists information about the Facebook user’s status of their Current City, Hometown, Sex, Birth Dates, Views and more. ProxySG provides an easy way to stop a Facebook user from updating their profile. A rule is created under the Visual Policy Manager in a Web Access Layer rule, where the destination field object you would add a Request URL Object to block access of the URI: /editprofile.php. The action would be that of Deny. Example:

![Figure 14](image)

Once this policy applied, the user is unable to post profile updates and only sees an hourglass on their browser. To avoid user frustration and help desk calls, appropriate warnings and exception alerts should be provided.
Summary

Blue Coat’s layered defenses help organizations provide safe social networking by blocking web threats, protecting sensitive data, improving user productivity and providing visibility and reporting into Facebook and other social networking web applications. Web gateway users benefit from all the layered defenses and policy controls noted above, while remote users with ProxyClient benefit from the WebPulse cloud community and real-time web rating services, as well as reporting and dashboards in Reporter 9. As a result, Blue Coat delivers a layered defense system that is unmatched in accuracy, relevance and timeliness.