LIVING WITH SOCIAL MEDIA
Secure and control social media and the Web 2.0 world
Secure and control social media and the Web 2.0 world

The Situation
You are close to maxing out your bandwidth and your network seems sluggish. You constantly have to rebuild workstations due to malware infestations. Upon further investigation, you discover that a user clicked on a shortened URL in Twitter that led to a nefarious site serving up malware.

As you walk around the office, you observe that more than half of the workers are watching breaking news videos about the death of a celebrity.

Your CFO receives a Facebook invitation from a friend, clicks on the link, and is redirected to a bogus site that installs keylogging software on his computer. You do not find out about it until an audit shows an offshore hacker has siphoned money out of your company’s bank account.

Driving Concerns
You would love to block all social media sites. The last thing you need is for your company to be the next headline, or worse, face lawsuits because of an attack that compromises your customer data.

But social media is here to stay. Full stop. You need to find a way to live with it.

Your conundrum is that conventional URL filtering solutions for controlling social media and other web use only filter URLs by category. They either block or allow the entire category—without granularity or exceptions.

Alternatively, there are secure gateway systems that go beyond URL filtering to let you lock down social media applications, preventing things like playing games, chatting over IM, and posting company specific information, or worse, uploading internal company documents. They can also help you track and report on web usage for HR concerns and capacity planning. However, these solutions may not help with:

• Bandwidth consumption. Although bandwidth has become less expensive over the years, the utilization has gone way up as the network supports critical services such as Voice over IP (VoIP) traffic and videoconferencing, not just web use. Sure, you have QOS set up, but you just do not need the added clutter of your employee base using YouTube unnecessarily or watching college basketball in March. And, unfortunately, in the dynamic Web 2.0 world, caching is no longer a viable option for reducing bandwidth consumption, with hit rates at14 percent or lower.

• Productive use of time. Managers are always looking for new ways to improve employee productivity. Having the ability to control functionality within social media sites gives management just that: The ability to block the games, chat, and other applications in Facebook, for example, can greatly help a manager focus a workgroup. Restricting use can also keep employees from installing malware that the administrator then must spend time cleaning up—reimagining the desktop and more.

• Controlling non-HTTP(S) traffic. You need to control port-agile applications (such as Skype, many IM clients, and P2P) that are not restricted to ports 80 (HTTP) or 443 (HTTPS). Nefarious, port-agile malware will also attempt to phone home on ports other than 80 or 443. Visibility and control over these ports typically require a firewall.

Beyond usage, you need to tackle the complex issues of malware and threats enabled by the evolving technology and exploding use of social media:

• Prominence of malware. Social media sites have become a gold mine for attackers.

  » URL shortening, popular with Twitter users, has made it possible for attackers to disguise the actual URL they are trying to get the victim to click. A user cannot simply mouse over a short URL to see and validate the actual URL.
Both Facebook profile spoofing (fake friend requests) and profile hijacking elicit participation in fake polls and questionnaires that serve as fronts for sites containing malware. Worms, such as Ramnit, spread when the hacker uses a victim’s account to post links to malicious sites on the walls of the victim’s friends. When the friends visit the site, a worm downloads and is used to steal login credentials. The attacker is rewarded because people often use the same login and password for social media as they do for their financial sites. Two-factor authentication processes on a banking site will ask for a user’s login and password, and the attacker will provide the correct information gleaned from the other site. The attacker appears to be the legitimate, authenticated user and drains the account.

In a similar IM money transfer fraud, a user thinks they “friend” a real person, when in reality they friend a spoofed profile or hijacked profile. Eventually, the user gets an urgent Facebook instant message that the “friend” is stuck in a foreign country, their wallet or purse has been stolen, and they need the prey to wire money quickly. The naïve user who does not validate the request out of band will send funds to the crook.

Facebook apps can deliver malware. A recent “Facebook Shutdown” scam spread by claiming that Facebook would delete all inactive accounts except those that confirmed via app installation.

Signature based scanning alone is no longer sufficient against dynamic, zero-hour attacks hosted in the websites of the Web 2.0 world

Social media sites may host malware that will use ports other than the traditional web ports (80 and 443), bypassing web-based controls

- **Filtering HTTPS content.** Most social media sites have an optional HTTPS version that allows traffic to bypass—and avoid filtering by—proxy and application control products. Malware and inappropriate use in this encrypted traffic would go undetected.

- **Potential for data leakage.** Posting information to social media sites is great for the work/life balance of employees, but can endanger a business if the employees discuss confidential company information. You should also worry about employees posting to wikis and blogs, or uploading data to cloud backup sites. Spear phishing and other social engineering attacks may use social media as the channel to elicit and exfiltrate your company’s intellectual property. While you cannot use technology to thwart social engineering attacks, you can use it to block the associated data theft.

You must overcome these challenges in order to balance the business drivers of allowing social media on your network against the very real resource usage and security concerns that result from doing so.

**Solution Description**

To meet the business requirement of allowing social media, both securely and with controls, McAfee recommends a layered approach including firewall and data loss prevention (DLP) built around a solid web proxy solution. A next generation web proxy is much more than a caching server with generic URL filtering. It can scan for malware and control applications on both HTTP and HTTPS. This combination addresses both the security and control requirements of social media:

- **Bandwidth concerns.** Allowing sites such as YouTube does not mean you have to allow every section of YouTube. A good proxy environment can allow you to exert fine-grained controls over social media site use. An effective solution might permit users to view company-specific videos, such as those used for training, but:
  - Block other sections of the site
  - Block other sections of the site during certain hours
  - Configure quotas for those other sections of the site
  - Limit certain user groups from accessing the other sections of the site through integration with Active Directory (AD), LDAP, or some other user identification
  - Throttle the bandwidth to the site

**Decision Elements**

These factors could influence your architecture:

- Do you have an existing proxy or URL filtering solution in place?
- Is your AD or LDAP environment robust enough to handle the added queries of an integration?
- Do you have a method for pushing proxy settings and certificates to the browser?
• **Productive use of time.** The same flexible rules used to manage bandwidth can help you limit use of applications and games in Facebook or Facebook chat to those required by business. You can also set up rules based on an application’s reputation and risk. By limiting use of risky and undesirable functions, you will reduce the malware introduced into the network and your team will spend less time reimaging infected systems.

• **Prominence of malware.** A next generation web proxy behind a firewall will allow you to scan for malware in every web request, including the transfer of files through IM and other social media applications. The proxy must be able to scan a page proactively, without the use of signatures, analyzing the anticipated behavior of the code executing in the web page. The proxy solution should also allow the ability to block downloads of certain media types and scan content to confirm that the media types are genuine.

• **Filtering HTTPS content.** When you make the decision to allow social media on your network, you must decide to filter HTTPS as well. If you can unlock encrypted traffic, you can enable HTTPS content inspection for use with data loss prevention (DLP), antimalware scanning, and company policy enforcement. A modern web proxy solution will have the ability to filter SSL content. It will also verify that the traffic is RFC-compliant HTTPS and not a piece of malware trying to phone home over port 443, as Operation Aurora did. A modern proxy solution will also verify that the certificate is not only valid, but is neither self signed nor expired (common attributes of malware). It should go farther and actively enforce certificate validation, as most users will ignore certificate errors and click through to a bad site.

• **Potential for data leakage.** The solution should provide the option to use on-board DLP within the proxy environment or off load this process to a full-blown DLP solution for in depth scanning and fingerprinting. A full DLP solution may be needed to satisfy compliance or regulatory requirements and should provide built-in policies and rules for common regulatory requirements, including PCI, GLBA, HIPAA, SOX, personally identifiable information, patient health information, SSN, CCN, stripe data, financial information, and more. A full DLP solution also includes built-in policies for intellectual property assets (such as source code, internal memos, product documents, and pricing information).

**Technologies Used in the McAfee Solution**

The McAfee solution has three primary components, McAfee® Web Gateway (MWG), McAfee Firewall Enterprise (MFE), and McAfee DLP Prevent, plus optional integration with McAfee ePolicy Orchestrator® (McAfee ePO™) and other McAfee solutions for endpoint protection.

McAfee Firewall Enterprise (MFE) serves several functions in this solution. First, it creates the DMZ that contains McAfee Web Gateway. The firewall should be configured to only allow traffic to come from the McAfee Web Gateway appliance over port 80 (HTTP) and port 443 (HTTPS). This restriction prevents an end user from circumventing the McAfee Web Gateway proxy solution. McAfee Firewall Enterprise also provides an application control solution called AppPrism®. In this deployment, AppPrism acts at the firewall to help control and filter applications using ports other than 80 and 443 (the traffic going through the McAfee Web Gateway).

The next piece of this solution is McAfee DLP Prevent, used to detect transmission of company-sensitive documents and communications. You should configure DLP Prevent as an Internet Content Adaptation Protocol (ICAP) server to accept traffic from McAfee Web Gateway, which you configure as an ICAP client. This arrangement allows you to create rules in McAfee Web Gateway to route either all or selected outbound traffic to the DLP Prevent appliances for scanning.
McAfee Web Gateway

McAfee Web Gateway (MWG) is a full-featured web proxy appliance that will filter, among other protocols, HTTP and HTTPS traffic. Like other proxy solutions, McAfee Web Gateway utilizes URL filtering to block social media categories such as games on sites like Facebook, or even block Facebook altogether using the category “Social Networking.” However, MWG goes a step further and blocks or permits based on dynamic reputation using McAfee Global Threat Intelligence™ lookups.

Reputation-based assessment is important since a site may be properly categorized as “social networking,” for example, but have a high risk reputation because it serves up malware. Most traditional URL filtering would allow such a site if the enterprise allows the social networking category.

In addition to URL filtering, MWG includes application category and reputation as part of its application controls. This functionality applies reputation-based filtering to the application itself (is this application risky?) and allows disabling of certain functionality within sites, such as photo upload in Facebook or mail in LinkedIn. With MWG, we apply McAfee AppPrism technology to ports 80 and 443 and take advantage of additional control options for fine-grained rule creation. You could create rules such as:

- Ensure only certain groups may upload photos, and only at certain times of the day
- Set quotas that limit users to one hour on social networking sites within a 4 hour viewing window
- Throttle the bandwidth users have to upload photos
- Direct user group traffic through McAfee DLP Prevent to make sure approved users are not uploading photos of intellectual property (perhaps a super-secret prototype)
An enterprise may also want to take social media application control a step further and actually remove functionality completely from a given site utilizing the HTML opener feature in the McAfee Web Gateway. HTML opener can scan a web page for defined tags, elements, and attributes and take a specific action. For example, one could scan for any page elements that contain YouTube videos and replace each video with a block page instead, effectively preventing users from watching YouTube videos.

The McAfee Web Gateway enables further control through integration with external identity and security infrastructure such as AD/LDAP, NTLM, eDirectory, Kerberos, cookie, client certificates (x509), CAC Card, or IP range. For example, you may have Twitter locked down to “read only” for the company as a whole, but you would like sales executives to have the ability to post things to Twitter as part of a sales campaign. You can implement this selective control easily if the sales executives are in their own AD group by allowing this exception in the Web Gateway rule set. Another example would be to use MWG rules and AD integration to allow LinkedIn use on your network, without letting the engineering group send code or other company intellectual property to a LinkedIn contact. You can create a rule specific to the engineering group and the LinkedIn site to route all of that outbound traffic through DLP Prevent first.

As the final layer of protection, the McAfee Web Gateway provides in-depth, zero-day active protection against viruses, worms, Trojans, and spyware at the Internet gateway. This extra layer of malware filtering at the gateway utilizes the McAfee Gateway Anti-Malware, or GAM, engine and real-time McAfee Global Threat Intelligence file reputation look-ups. Instead of matching signatures, the GAM engine emulates and analyzes the site’s intent before the page renders at the end user’s desktop. This file-agnostic content inspection is able to unveil and strip out various web attacks, including embedded code, buffer overflows, and other exploits, protecting the desktop before damage is done. To maintain its zero-day detection accuracy, McAfee Gateway Anti-Malware Engine updates continually via the McAfee Global Threat Intelligence network.

McAfee Firewall Enterprise

At an architecture level, the firewall creates a DMZ and forces all port 80 and 443 traffic through the McAfee Web Gateway. In addition, the McAfee Firewall Enterprise (MFE) performs application detection, or identification, for all other ports. This system improves application control and adds a layer of defense. You also gain visibility into applications in use on the network.

AppPrism uses many mechanisms to identify what applications are traversing the Firewall. First, it classifies traffic based on Port and IP address. Encrypted traffic may be decrypted and inspected as well. Signatures are then applied to the traffic to determine the application, and policy is applied. Application discovery allows MFE to determine the application regardless of port or protocol.

In most cases, AppPrism also identifies default or expected ports for the application. This function serves as application defense by controlling, or blocking, port-agile applications such as Skype. For example, once MFE detects that an application is Skype, MFE can force Skype to use a specific port. MFE can also block certain users from using Skype all together. This functionality can be configured via an access control policy. Access control policies are specific to your source, destinations, zones, applications, and optionally user or user groups. You can have multiple policies based on any of these criteria. For example, a rule might say that if you are a member of the AD user group “administrators,” you can access Skype. If this rule were not true, the firewall would attempt to match other rules lower down the list. Perhaps executives in North America can also use Skype. Eventually, a non-administrator, non-executive user might hit the default rule to “deny all.”

Applications can also be enabled on a per zone basis. Rules determine additional controls such as a feature within the application you want to disable. For example, in Yahoo Messenger you may want to allow chat, but block file transfers for some groups. For other groups that may transfer files, you might add other MFE security features such as antimalware scanning. This would allow you to ensure inbound FTP transfers did not carry malicious content.
McAfee DLP Prevent

McAfee DLP Prevent is part of the larger suite of McAfee Data Loss Prevention products. McAfee DLP Prevent communicates via ICAP, or Internet Content Adaptation Protocol, to the McAfee Web Gateway to perform detailed content inspection. This configuration allows the added protection of scanning outbound communications transmitted through social media sites and other web applications. If it detects a policy violation, DLP Prevent can, at your choice, encrypt, redirect, quarantine, or even block the data transmission in question.

Your enterprise may want to scan for specific number patterns such as social security numbers or credit card numbers. McAfee DLP Prevent has built-in policies and rules for common regulatory requirements, including PCI, GLBA, HIPAA, SOX, personally identifiable information, patient health information, SSN, CCN, stripe data, financial information, and more. McAfee DLP Prevent also provides built-in policies for intellectual property assets (such as source code, internal memos, product documents, and pricing information). Using comprehensive data classification, DLP Prevent automatically identifies and protects more than 300 different content types (including complex computer aided design (CAD) files) in over 13 languages. You may fingerprint documents that contain intellectual property and scan traffic for these fingerprints.

Optional Integrations

You can integrate this solution with McAfee ePolicy Orchestrator (McAfee ePO) for viewing dashboard status information, such as the top blocked sites. McAfee ePO may also be used to configure policies for McAfee DLP Prevent. This solution may also dump logs to a syslog server, where they may be imported into McAfee Enterprise Security Manager (ESM). McAfee DLP Prevent may also be used with email gateways, such as McAfee Email Gateway, for consistent application of data loss prevention policies.

Impact of the Solution

Deploying McAfee Web Gateway in conjunction with McAfee Firewall Enterprise and McAfee DLP Prevent will give your enterprise peace of mind as you safely allow access to social media sites. Your enterprise will be able to reduce its bandwidth consumption by limiting the use of sites such as YouTube, or by throttling the bandwidth of these sites at certain times of the day, and by user criteria.

By preventing malware at the gateway, you capture an additional return on this investment. Your IT staff will not have to spend time reimaging workstations. You will also greatly reduce the number of connections through your firewalls, reducing the amount of firewall hardware required to scan the remaining “good” traffic.

With these controls and security features, even if an employee is duped by a clever social engineering scam or shortened URL, you will have a solid line of defense to protect that user as well as your company and its data.

Q&A

What other ports does the McAfee Web Gateway filter?
In addition to ports 80 (HTTP) and 443 (HTTPS), McAfee Web Gateway will also filter FTP, and IM traffic including Yahoo, Windows Messenger, ICQ, and XMPP.

What other products are available in the DLP solution?
In addition to DLP Prevent, McAfee offers DLP Monitor for analyzing data in motion across the network, DLP Discover for finding sensitive information at rest by crawling repositories in the enterprise, and DLP Manager for centralized management of all three products and integration with ePO. Host-based DLP offers policy-based controls and content filtering for endpoints that will remain in effect even if the endpoint leaves the network.
Do I have to rip and replace my current infrastructure to implement this solution?
No. It is very common to follow a phased approach in migrating to a new web security solution. Here are three equally legitimate paths:

• The McAfee Firewall may be installed as a new DMZ first, with Web Gateway and DLP added afterwards.
• If you already have a DMZ and web proxy environment, McAfee Web Gateway can be configured in a proxy chain (next hop) so that an existing proxy environment continues to run while the MWG environment is configured. Once McAfee Web Gateway has been installed and configured, McAfee DLP may be added as a second phase.
• Alternatively, once a DMZ is in place, DLP integration can be a first phase, with ICAP filtering configured off an existing proxy solution. The McAfee Web Gateway can then be deployed in a proxy chain as in the previous example.

How do I get visibility into social media traffic to see what end users are doing?
McAfee Web Gateway integrates with McAfee Web Reporter, which produces detailed reports on all web traffic. You can set up delegated reporting as well. This option allows HR or other department heads to run their own reports without asking IT for each edition. Similarly, McAfee Firewall includes the McAfee Firewall Reporter, which provides detailed reports on all firewall traffic. McAfee DLP Prevent has the ability for customized views and incident reports with both summary and detailed views of security incidents and the mediation actions taken. With all of the products, you can also write to a syslog server that can then be imported into McAfee Enterprise Security Manager.

Additional Resources
www.mcafee.com/web-gateway
www.mcafee.com/firewall-enterprise
www.mcafee.com/data-loss-prevention
www.mcafee.com/epo
www.mcafee.com/producttrials

About the Author
Bob Wicklund is an enterprise solution architect for McAfee Cloud and Content Security. He has been in the IT industry for nearly 20 years, 15 of which have been in the enterprise software space with companies such as Stellent, Oracle, Secure Computing, and McAfee. He has designed and implemented some of the largest web and web security deployments at companies such as Procter and Gamble, New York Times, State Farm, Oracle, and Boeing, as well as local, state, and US Federal governments. Bob has presented at many user conferences, including every McAfee FOCUS user conference.