A Websense® White Paper

Implementing Best Practices for Web 2.0 Security with the Websense Web Security Gateway

websense®
ESSENTIAL INFORMATION PROTECTION™

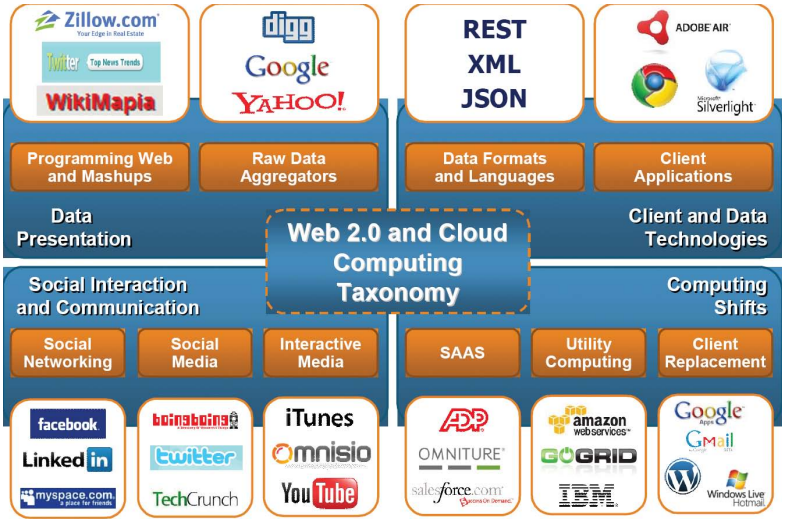
Table of Contents

Introduction

IDC, one of the premier industry analyst firms recently published a white paper outlining "Best Practices for Securing Web 2.0." In this white paper, sponsored by Websense*, they list 10 specific practices organizations should consider for getting the most from this new technology with minimal risk. This paper examines how you can quickly and easily implement these best practices in your organization using the Websense® Web Security Gateway.

The Websense Web Security Gateway offers unique capabilities that enable organizations to take advantage of the latest technologies to improve their business processes while maintaining security, accountability, and visibility for all of the stakeholders in an organization.

Web 2.0 is the current label for the latest generation of Internet-based applications and Web sites that contain user-generated content combined with rich media delivery technologies. While social networking sites are the most commonly recognized and discussed Web 2.0 properties, in fact Web 2.0 technologies also encompass a broad range of sites, like Google and services such as SalesForce.com which are in common use by companies and organizations of all types and sizes today. One of the fundamental properties of Web 2.0 is its ability to deliver real-time, user-generated content in new and more powerful ways than traditional Web 1.0 sites that deliver static content. Examples of the broad range of applications and technologies currently in use are illustrated in the following diagram.



Web 2.0 Taxonomy

While many of these new types of Internet technologies are in wide use, the ability to secure and control their use is not as widely deployed. Many of the traditional IT security and control technologies simply do not address the risks associated with accessing dynamic content in real time via these new delivery systems.

- Network firewalls provide little protection as Web 2.0 relies primarily on standard HTTP and HTTPS protocols that simply can't be blocked without cutting off Web access.
- Traditional antivirus is limited to inspecting file transfers, and many of the greatest "drive by" threats encountered today are contained in browser scripts that are invisible to AV.
- Web reputation services alone are ineffective as some of the most valuable sites on the Web, such as Google or Yahoo, have fallen victim to hosting malicious code, and simply blocking access to these sites is not an acceptable answer for most businesses.

*Source: IDC White Paper sponsored by Websense, Best Practices for Securing Web 2.0, Doc # 218589, June 2009

- Simple URL filtering that blocks objectionable or time-wasting content based on the home page address of the Web site no longer works when sites now commonly aggregate information from multiple sources.

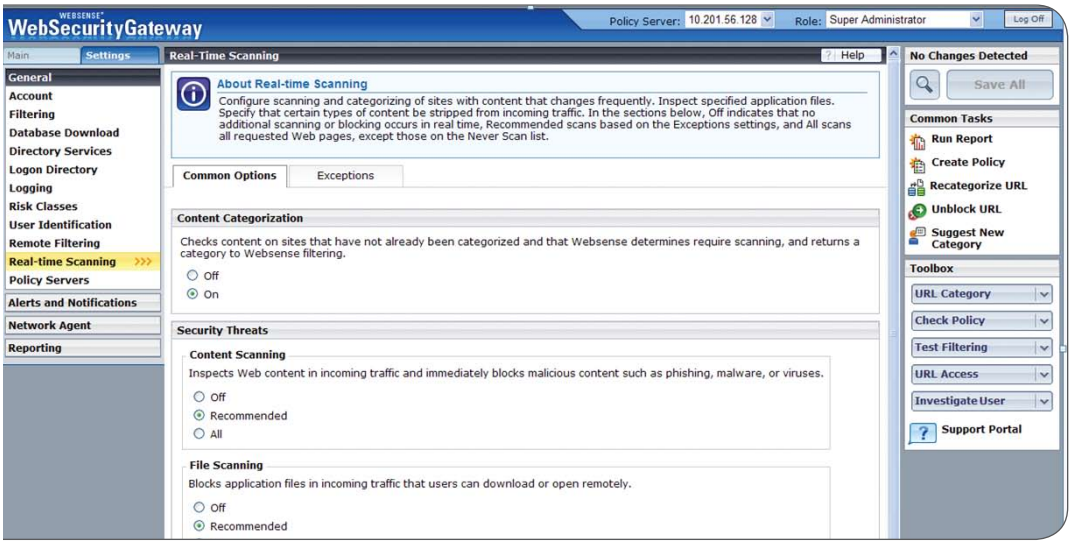
The way to address Web 2.0 threats that combines the best aspects of traditional security and control techniques is with new technology designed specifically to address the dynamic, real-time nature of Web 2.0. This paper describes how the Websense Web Security Gateway enables you to quickly and effectively implement a best practices approach to making Web 2.0 secure and effective.

Implementing Best Practices with the Websense Web Security Gateway

While there are many ways to address the different aspects of Web 2.0 security some key elements have emerged that deliver the best level of protection and control for the least cost and effort. The following sections outline how you can implement these practices in your organization with Websense.

Protect your organization:

"IDC strongly urges organizations to create a security strategy that empowers and encourages workers to innovate with Web 2.0 rather than hinders such efforts." *



Websense Web Security Gateway

Enable both real-time content and security scanning on all categories of Websites that leverage user generated content from search engines and Webmail to social networking.

With the Websense Web Security Gateway management system, enabling advanced real-time content scanning requires three simple clicks to fully enable protection.

The system automatically recognizes sites containing dynamic content or potential threats and applies the results of the real-time scan to policies configured by the administrator. This level of automation decreases the risks of human error and enables the administrator to focus on the business results desired.

*Source: IDC White Paper sponsored by Websense, Best Practices for Securing Web 2.0, Doc # 218589, June 2009

Website Mashup Example

Real-time scanning enables "good" information to be displayed and "bad" information or malicious content to be blocked on Web 2.0 sites using aggregated content.

This capability is the key element that has been missing from the traditional security world and is the cornerstone in enabling you to say "Yes" to Web 2.0 safely and productively with Websense.

Enable Web 2.0 benefits:

> "The Web2.0@Work survey found that 86 percent of IT managers feel pressure to allow access to Web 2.0 sites and applications from within their organization and that 30 percent of this pressure is coming from C-level and director-level staff. Organizations need the tools to embrace Web 2.0 technologies while ensuring security and compliance." *

Use drill-down reports to determine which users and groups consistently access Web 2.0 technology.

Web usage patterns in your organization can be determined by simply clicking on the "Top Categories" chart on the real-time dashboard display. Integrated drill downs simplify navigation and enable powerful, yet easy to use reports.

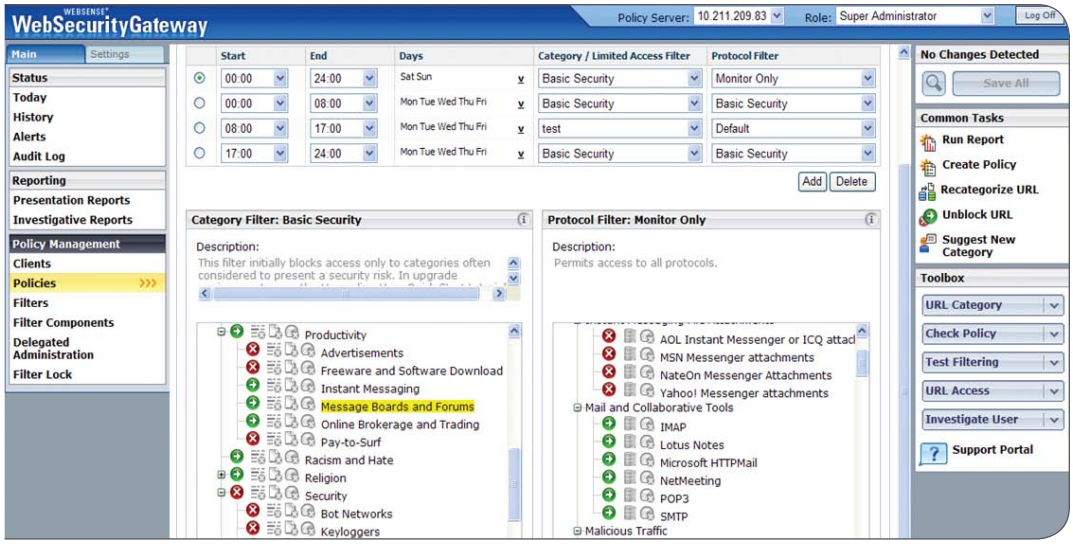
Websense Web Security Gateway fully integrates with the leading directory systems like Microsoft Active Directory and LDAP to provide actionable information on individual users as well as organizational groups. Knowing what Web 2.0 properties your marketing group uses versus what the needs of your finance group are enables you to develop and apply polices appropriate to each groups needs. No longer are you forced to take a one-size-fits-all approach to Web 2.0.

Create a policy to enable safe and appropriate use of Web 2.0

Websense provides the industry's only unified policy management system that enables you to manage all aspects of your users' security, Web access and application control from a single screen.

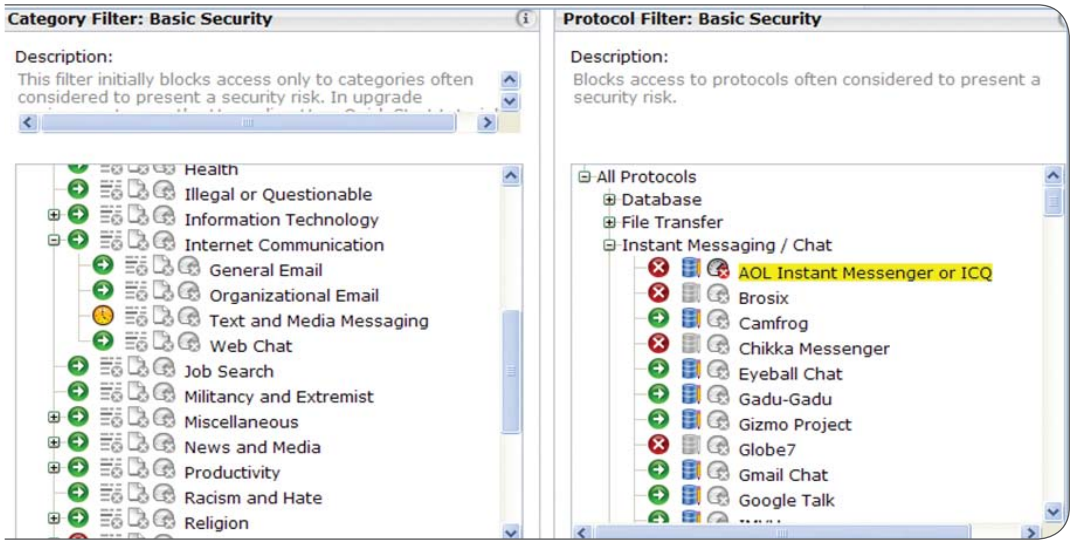
Web security and site content types are categorized in the left-hand pane. You select categories such as "Malicious Web Sites" or "Spyware" from the security categories to enable protection. Categories your organization deems inappropriate or non-productive such as "Pornography" or "Shopping" can be selected for filtering in the same area.

*Source: IDC White Paper sponsored by Websense, Best Practices for Securing Web 2.0, Doc # 218589, June 2009



Websense Web Security Gateway Policy Configuration

Integrating security, acceptable use and application control polices across all protocols from a central point decreases management time, minimizes errors and makes applying technical controls to organizational policy much simpler.



Websense Web Security Gateway Website and Protocol Categories

Increase Productivity:

> "Web 2.0 applications and newer instant messaging tools leverage evasive techniques to communicate and share information." *

Control specific applications like instant messaging over the Web by users with measures like time allotment, bandwidth-based controls, or content restrictions.

Control of Internet applications like instant messaging and peer-to-peer has been one of the biggest challenges to network security. Increasing workforce productivity by enabling control and auditing of Web 2.0 tools without the need for additional point products or staff is an easy win for any organization.

*Source: IDC White Paper sponsored by Websense, Best Practices for Securing Web 2.0, Doc # 218589, June 2009

Websense Web Security Gateway recognizes and controls more than 125 separate network protocols that are used by literally thousands of applications and enables full control and auditing of the usage of these tools within the organization.

The right-hand pane (Protocol Filter) of the unified policy manager contains categorized lists of non-HTTP(S) applications and their associated protocols. These applications are identified "on the wire" via network application fingerprinting technology regardless of the TCP port used. Applications and attachments can be blocked, allowed or limited to control their impact on network resources.

Applications that use or tunnel over HTTP and HTTPS are contained within the left hand pane (Category Filter) and include advanced controls to allow "Quota" access for a predefined amount of time and "Confirmed" access that requires users to explicitly acknowledge their intent to access a site. A full range of protocol controls is included and all applications can be logged for auditing and reporting.

Get Full Visibility:

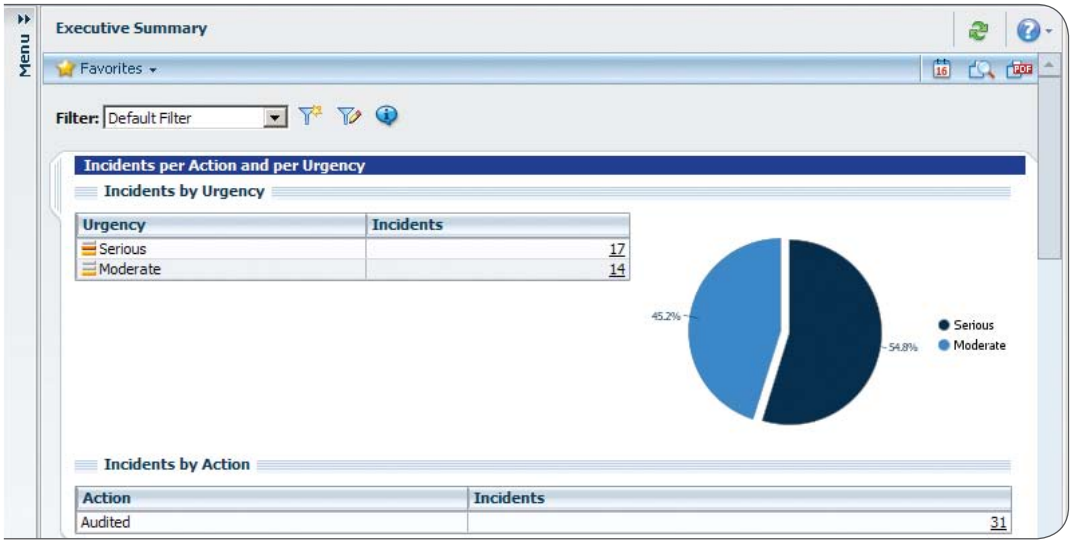
Decrypt and examine the content including data for all HTTPS traffic to Web 2.0 sites and for applications like Webmail for inbound threats and outbound risks.

Websense Web Security Gateway includes a full featured HTTPS proxy that is simple to use while incorporating a full range of controls. Policies are generated using the unified policy management system and are automatically applied to protect and control encrypted traffic

Protect your Data:

> "A recent IDC survey on information protection and control (IPC) showed that Web email or Web posting (e.g., message boards, blogs) accounted for 37 percent of information leaks." *

Monitor and report on sensitive and regulated data sent over or posted via the Web by users, intended destinations, and the category of site or Web application.

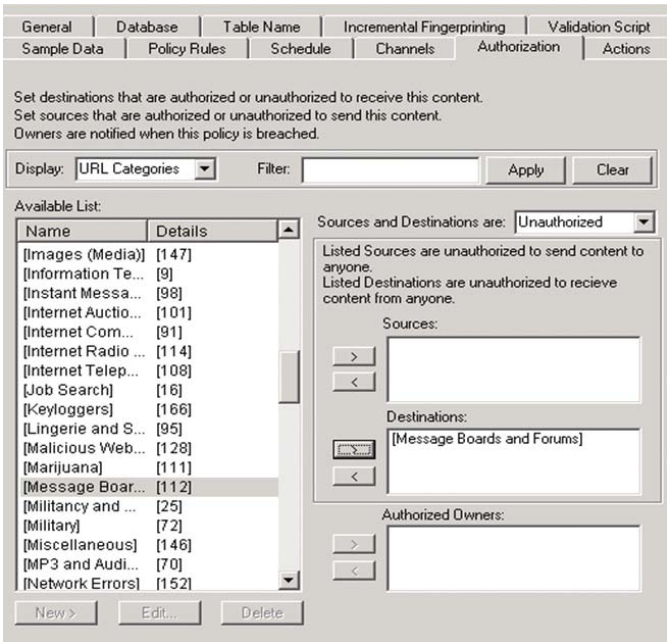


Websense Data Security Executive Report

Protecting against the loss of confidential data via Web 2.0 properties requires a fully integrated DLP and Web 2.0-aware Web gateway.

*Source: IDC White Paper sponsored by Websense, Best Practices for Securing Web 2.0, Doc # 218589, June 2009

Protecting against the loss of confidential data via Web 2.0 properties requires a fully integrated DLP and Web 2.0-aware Web gateway.



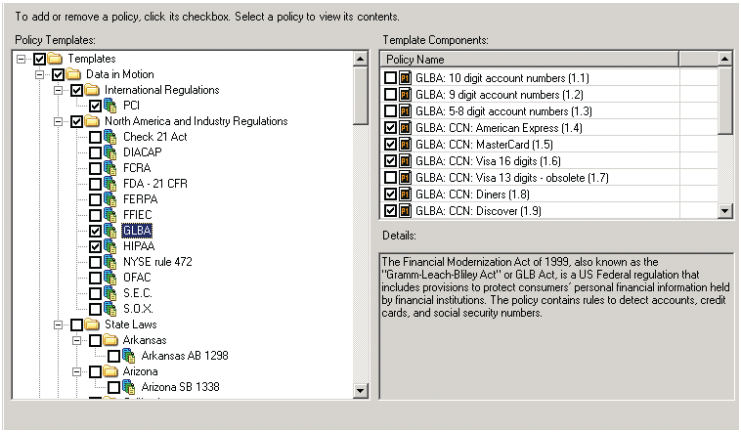
Websense Destination Awareness Configuration

Websense data security solutions integrate seamlessly with the Websense Web Security Gateway to provide full visibility into all Web communications, including encrypted sessions.

This integration enables unique capabilities, such as full intelligence into the location and category of Web site or application the user is accessing with full audit and detailed reporting capabilities.

Websense data security leverages the directory integration and user authentication capabilities of the gateway ensuring full linkage between the monitored session and the user.

Then, create the appropriate enforcement policy that protects and enables the organization.



Websense Data Security Policy Wizard

The data security extends the capabilities of the solution to provide full enforcement capabilities for both encrypted and clear text Web sessions. Over 950 templates are provided to help ensure compliance with a wide range of regulatory and compliance templates.

Implementing data protection for your organization simply requires the selection of the appropriate template and the user, or group of users the protection should be applied to.

Summary

In summary the development of Web 2.0 has ushered in a new era in how organizations communicate and do business. Many organizations have been concerned about embracing the competitive advantages Web 2.0 can bring due to concerns about security, control and the loss of sensitive information via these new technologies.

Websense has developed a new generation of technologies targeted directly at enabling the safe and effective use of Web 2.0 with minimal risk. Customers can implement the best practices outlined within this document to address the concerns they have and say "Yes" to Web 2.0 with confidence.

About the Websense Web Security Gateway

The Websense Web Security Gateway enables organizations to accelerate business by fully utilizing the capabilities of the Internet without having to worry about security, productivity, and liability threats such as malicious and inappropriate content and data loss. As the Internet evolves from a static, known resource to supporting dynamic and user-generated content such as wikis, blogs and other content sources, so the methods of enforcing policy and security also need to evolve.

How the Websense V10000™ works

The Websense Web Security Gateway takes the expertise, knowledge and capabilities of the Websense Security Labs™, and incorporates that inside the product. The Websense Security Labs continuously monitors the changes of the Internet, and has developed specific algorithms and analytic engines that can analyze Web content—including dynamic, user-generated and personalized content. It is these analytic engines that power the control over dynamic and previously unseen content, as well as detecting the intent of dynamic scripts and other active web elements to prevent malicious behavior.

By sitting in line with network traffic and utilizing the integrated Web proxy capabilities, the Websense Web Security Gateway has complete visibility into Web and network traffic in real-time. This enables the Web Security Gateway to analyze Web content as it is being accessed—passing content through the real-time analytic engines. These analytics examine all elements of the Web content to apply policy and determine if content is appropriate or not.

There are several capabilities that a Web security solution must have to be truly effective today:

- Visibility into all Web traffic, whether it is encrypted or not
- The ability to identify dynamic and previously unseen Web content in real-time
- The ability to analyze the action and intent of active scripts that might be malicious
- Broad control over network applications
- Flexible policy creation
- Granular, actionable reporting

The Websense Web Security Gateway is the leading solution to offer these capabilities, helping ensure users remain secure and productive while accelerating their business through the use of the Web.

© 2009 Websense Inc. All rights reserved. Websense is a registered trademark of Websense, Inc. in the United States and certain international markets. Websense has numerous other registered and unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners. 06.26.09