GFI White Paper

To block or not to block - why web filtering is no longer a taboo

The way we use the Internet has fundamentally changed in the last 20 years, driven by the introduction of the World Wide Web. The way the web has reshaped how we use the Internet and how we deliver content to users is phenomenal and has far exceeded the original expectations of its creator, Tim Berners-Lee.

GFI®

Contents

Introduction

However, the ubiquity of the web and its ability to display and deliver such a broad range of content brings with it significant challenges for organizations, particularly for those looking to maintain productivity and ensure that working environments are not compromised by inappropriate Internet use and unintended exposure to offensive or malicious material. Research by IDC shows that up to 40% of employee Internet activity is non-work related, illustrating the level of risk to the organization from idle browsing during the working day.

Clear and effective policy on Internet use is a critical component of a strong and all-encompassing IT security strategy. It is also essential in ensuring that employees follow best practices when using the Internet at the workplace. However, Internet use policy must be supported by effective technology to enforce the policy and to protect users as well as the organization itself from the follow-on effects of accessing inappropriate web content in a work environment.

Web filtering plays a key role in enabling organizations to limit web activity at the workplace, not just to prevent idle or unauthorized web browsing, but also to protect users and their computers from intentional or inadvertent exposure to IT security threats such as malware and scam websites. Content filtering and control is also essential to ensure that companies are not unduly exposed to legal challenges resulting from inappropriate use of the web at the workplace, while allowing them to effectively manage bandwidth and network capacity by looking at which websites and services are used and when, assisting in capacity planning and highlighting network traffic issues before they become systemic.

The taboo of web filtering

Technology can be used to limit what sites users can access at the workplace. This has clear benefits for the organization; and today's web filtering technology is both well-developed and extremely reliable, ensuring predictable and consistent results, while at the same time minimizing the instances of inaccurate content blocking and ensuring that deployments are straightforward and easy to maintain.

However, use of technology to prevent web access is considered among some end-users as ideologically sensitive due to the fact that it counters the original purpose and aims of the Internet and the World Wide Web.

This perception of the Internet as a free and unrestricted platform is widely considered invalid by many Western governments, who have already been placing limitations on Internet access and implementing laws that determine the legal and illegal dissemination of information online . The goal is largely to combat the flow of material such as pornography but also, with regard to the distribution of classified government data, prevention of unlicensed online gambling on the web, protection of intellectual property rights and more.

While the notion of a free and unimpeded Internet is a noble and commendable idea for individuals to support, organizations have much wider implications to consider when providing users with access to the Internet at the workplace. Organizations are liable for the activities of their employees, both online and offline, and thus have a duty of care to ensure that employees are not exposed, intentionally or otherwise, to material that could offend or be interpreted as offensive or which could leave the company open to prosecution or claims for compensation.

Indeed, for an organization, the taboos of restricting access to certain quarters of the web are far outweighed by the need to deliver a safe, inoffensive and culturally sensitive working environment.

Furthermore, early consumer web filtering applications – which were a very different and cruder form of technology from the enterprise applications we use today – often relied on keywords, rather than detailed and well-maintained lists of good and bad sites , in order to determine what should and should not be blocked, often with unfortunate results. Over-zealous and poorly-maintained implementations would see otherwise harmless sites, including national newspapers and broadcast news sites, being blocked along with popular web-based email services such as Hotmail, not on the basis of productivity or bandwidth concerns, but merely because these under-developed applications generated false-positives, mistaking perfectly legitimate sites as ones potentially containing offensive content .

Today, web filtering technology has moved far beyond these early pre-conceptions of technology, and deliver a compelling argument in favor of allowing companies to control how, when and what corporate Internet connections are used for ensuring that web access at the workplace is for the benefit of the organization and its employees

The benefits and importance of enterprise web filtering and content monitoring

Web filtering can deliver many positive benefits for both organizations and end-users that go far beyond the basic implementation of preventing access to named websites or particular types of websites. Filtering technology is predominantly a security tool, one that provides an essential layer of centralized, server-side protection from security threats before they manifest on client devices.

The benefits and capabilities of web filtering solutions fall into four areas:

- **Productivity** – Web filtering can allow an organization to address excessive use of non-work websites by either preventing or limiting access to services such as social networking, online auctions, online gambling, personal web-based email, celebrity gossip, torrents, file download sites and so on. This can be done in numerous ways, ranging from a total blockage of access requests, down to allowing specific users and work groups, or simply allowing access at certain times such as lunch time or before and after normal working hours. The latter approaches can help companies balance the needs and morale of staff while at the same time ensuring that day-to-day activity is not hindered by web-based distractions.
- **Minimizing liability** – Companies must take all reasonable steps to protect themselves and their staff from liability. For example, website content that seems funny to some may be considered racially or sexually explicit, offensive or discriminatory by others. Case law in several countries has confirmed that the employer is responsible for the web activities of its staff , particularly when these activities involve illegal or offensive material. By implementing web filtering technology, not only can an organization prevent access to much of this content before it is accessed, but through associated web monitoring technology, it can also maintain accurate and detailed logs to show who attempted to access inappropriate content and when, allowing appropriate action to be taken as necessary and for evidence to be produced to support claims of inappropriate IT use at the workplace.
- **Network and bandwidth management** – The changing nature of the way we use the web and the way content is expressed on websites is placing growing pressure on broadband connections both at home and at the workplace. Growth of video-on-demand sites such as YouTube, BBC iPlayer, Hulu and SeeSaw has triggered a substantial increase in bandwidth consumption. This is in addition to the increased use of video on everything from corporate websites to retailers to reference services. The result is that inoffensive casual browsing and even legitimate work-related browsing can place strain on both an Internet connection and the internal network. Web filtering and monitoring helps organizations understand the types of sites and content that is accessed at the workplace and at what time, helping with capacity planning and highlighting areas for further investigation in the case of casual browsing or upsurges in traffic around key events such as the Olympics, FIFA World Cup, major news events and other video-heavy content events.
- **Data security** – Web filtering delivers an essential layer of protection from malware, phishing and other online scams long before client computers and end-users would be exposed to them. By blocking access to known bad sites at source, end-users can be protected from straying into the path of malware and can avoid being duped by scams such as phishing attacks, while malware already present on devices can be limited in its ability to access the web to further infect a machine.

An effective solution for web filtering

Enterprise-grade web filtering solutions represent highly-developed and proven technologies for accurately blocking and allowing web access based on pre-determined lists of good and bad sites, as well as making

use of user-provided data and feedback on legitimate and malicious sites. Combined with heuristic scanning, these tools deliver a layer of protection that can stop security threats before they even have a chance to connect and load.

A robust solution will allow organizations to maintain highly detailed control over web access centrally, set and enforce policies on Internet usage, as well as provide a high level of web-based security – blocking malicious content before it reaches the user's machine.

Administrators should be able to see in real time what sites are being browsed and what files are being downloaded. An active connection, browsing session or download should easily be blocked, simply by clicking on a single 'block connection' button.

Filtering and access policies can be set based on user, work group and IP range, allowing highly granular control over who has access to what within the organization, while at the same time maintaining blanket rules over blocking and access limitations. Time and bandwidth-based web browsing policies can also be used to allow access at certain times, or for quotas to be allocated, particularly useful for allowing access to high-bandwidth sites such as YouTube, but capping exposure and maintaining a balance between bandwidth and free use of the organization's connection for work and non-work browsing.

Summary

Today's web-based threats from malware and other malicious websites alone make a compelling case for implementing web filtering and content monitoring at the workplace. While technology delivers significant security benefits, it offers much more to the organization at large and to the IT department in the form of providing a centralized way to monitor, analyze and limit Internet use as needed.

Client-based security solutions such as firewalls and antivirus solutions, regardless of how good they are, should not be expected to provide total and unwavering protection from threats. Rather, these should be paired with robust server-side web filtering solutions such as GFI WebMonitor™ to deliver an array of proven counter measures that can tackle Internet-based threats at all stages, not just locally on the client. Coupled with centralized management and control of both whitelists and blacklists, organizations can ensure that problematic or high-bandwidth sites are blocked, limited or monitored, as needed, to ensure the right balance between unencumbered Internet access and business productivity.

Web filtering plays a significant role in enabling what can and cannot be accessed. However, it is not about creating multi-tier access for gain or undermining net neutrality, but more about maintaining access integrity and ensuring security over needlessly limiting access to information.

In short, web filtering is no longer a taboo; it is an essential tool in the battle against IT security threats and an important resource for IT departments trying to maximize the performance and cost-effectiveness of networks and connectivity.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com