Top Seven Reasons for Web Traffic and Content Filtering

We all know the upsides and downsides to Internet access. So how do we get the best of both worlds? How do we capitalize on the upside while limiting the threats of wide-open internet access? The answer is simple: filtering content and web traffic.

Micro Focus provides you the ability to monitor, filter, and block HTTP traffic. Micro Focus integrates with compatible ICAP systems to provide content filtering for incoming and outgoing internet traffic, including URL filtering, social media, and search filtering. Micro Focus intercepts inappropriate or harmful content and alerts managers, administrators, and other pertinent parties via email and the Micro Focus interface.

Outlined below are the top four reasons to filter internet content and traffic in your organization:

1. **Prevention of Malicious Sites and Inappropriate Content.** Web traffic and content filtering allows you to prevent access to harmful and malicious content and websites while still providing your employees access to good, appropriate, and pertinent information. Unfettered internet access can lead to inappropriate, malicious, or harmful content. This can be in the form of malicious, dangerous, or pornographic websites, or it can be through the creation of harmful content, including social media, blog, video uploads, or other web postings.

2. **Avoid data leakage.** A mix of policy and technology is essential to combat data leakage. Monitoring and filtering what your employees share online will help enforce policy and prevent data leakage: confidential information, trade secrets, company processes, upcoming product releases and other organizational information others can glean from data your employees share. This data leakage can be inadvertent or deliberate; however, no matter how it happens, it will cause harm to your company.

3. **Managing Your Company Brand and Image.** Social media, video sharing, and other types of web sites give you the ability to promote your company and brand. These sites give you a quick and easy way to communicate with your customers, announce upcoming products, events and promotions, and promote your company and brand in innovative and exciting ways. However, with these benefits come risks, including damage to your company brand and image through employees posting negative, inappropriate, or confidential content in the company's behalf. To combat this, it is imperative that internet traffic is monitored to ensure that your employees are not engaging in harmful practices and your organization is protected from potential threats.

Examples of filtered content are:

- **Inappropriate or harmful communications**
- **Pornographic or illicit materials**
- **Advertisements**
- **Suspect information**
- **Other content based on school policy**

Secure Messaging Gateway stops cybercriminals, spam, and porn before they ever enter your messaging system. The Secure Messaging Gateway uses the latest technology to detect viruses, malware, spam, and illicit images and block them from your system.

www.microfocus.com

4. **Preventing Loss of Productivity.** Web filtering helps prevent productivity losses by preventing employees from accessing websites and applications that violate company policy or interfere with an employee's day-to-day responsibilities. One of the top managerial fears with open internet access at work is loss of productivity through cyberloafing. Online shopping, gaming, social media, and other personal browsing can sometimes win the work vs. play battle. Customer needs take a backseat to employees spending work time on personal applications.

5. **Internet Access Protection.** Micro Focus scans HTTP traffic from a compatible ICAP device and prevents access based on URL category, reputation, corporate policy, and file type, including hidden executable and malignant files. Web traffic monitoring and filtering will protect your organization from the inherent risks of internet usage, including:
   - Malicious sites
   - Loss of productivity from internet misuse
   - Inappropriate incoming and outgoing content
   - Virus infiltration

6. **More Than Just Blocking.** Micro Focus HTTP monitoring provides organizations the ability to filter content instead of just blocking it. This allows appropriate content from sites that previously would have been blocked in their entirety.

   Examples of HTTP Traffic Filtering Sites:
   - Facebook, Twitter, LinkedIn, and other social media
   - Google, Bing, and other search sites
   - YouTube, Vimeo, and other video sharing sites

   Allow employees to post and search good content by monitoring and filtering while protecting your organization from threats.

7. **Micro Focus® Secure Messaging Gateway.** In addition to web and content filtering, Micro Focus Secure Messaging Gateway protects vital business communication for thousands of organizations in industries such as government, education, financial services, healthcare, and business.

   Secure Messaging Gateway stops cybercriminals, spam, and porn before they ever enter your messaging system. The Secure Messaging Gateway uses the latest technology to detect viruses, malware, spam, and illicit images and block them from your system.

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com