

OPINION



By Eryin Halmen Country Manager of Malaysia & Brunei, Fortinet Inc

SECURING CORPORATE ASSETS with Web Content Filtering

THE WORLD WIDE WEB (WWW) has become a critical and integral part of modern business communications as well as a national pastime for billions of users.

With all of the good attributes of increased communications and productivity, the web has unfortunately become the new breeding ground for malicious activity. Its standards-based worldwide appeal and incredible number of applications has made it the medium of choice for modern hackers and thieves looking for new ways to disrupt services, steal information, and perform malicious activities for financial gain.

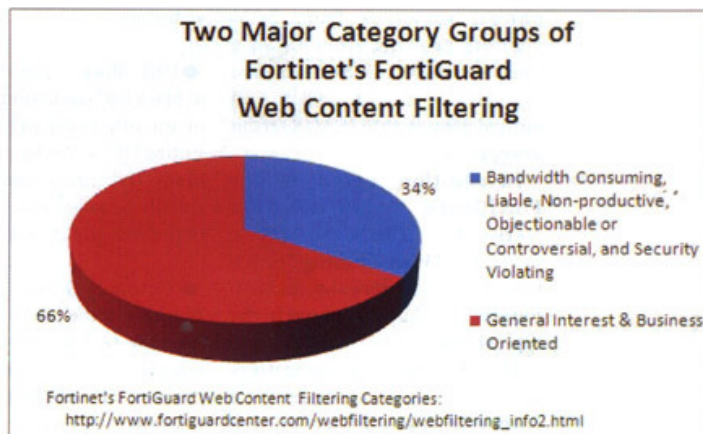
CONTROLLING WEB ACCESS

Along with the dramatic rise in the number and severity of security threats ranging from identity thefts, fraud and theft of credit card information, the need for web content inspection and filtering has increased manifold due to:

- Loss of productivity when employees are accessing the Web for non-business reasons.
- Network congestion - valuable bandwidth is being used for non-business purposes and legitimate business applications suffer.

- Increasing costs as more Internet bandwidth is added to support both legitimate and illegitimate business applications.
- Loss or exposure of confidential information through chat sites, non-approved email systems, Instant Messaging, peer-to-peer file sharing, etc.
- Increased exposure to web-based threats (viruses, worms, trojans, spyware, etc.) as employees surf non-business related web sites.
- Legal liability when employees

- access inappropriate and offensive material.
 - Copyright infringement caused by employees downloading and/or distributing copyrighted material such as music, movies, etc.
 - Negative publicity due to exposure of critical company information, legal action, etc.
- Worldwide government regulations on Internet access and information security are being enforced by many countries and individual states such as Sarbanes-Oxley, HIPPA and Children's Internet Protection Act (CIPA) for schools and libraries.



OPINION

The need to enforce corporate Internet Usage Policies requires the ability to monitor and block unauthorised web sites.

Out of the 40 million websites Fortinet's FortiGuard Web Content Filtering service covers, 34% are potentially bandwidth consuming, liable, non-productive, objectionable or controversial and security violating. This is a good one-third of the sites covered. In addition, to a certain extent, legitimate websites of banks, government institutions, service providers, online shops, etc. have been hacked or seen hosting malicious scripts that can automatically install Trojans into the Internet users' computers.

The need for complete content security is rising quickly as corporations are quickly realising that traditional security devices such as firewalls, IDS, and host based Antivirus are no longer protecting them from the new generation of threats.

Reports IDC show that the rise in the Secure Content Management (SCM) appliances (Antivirus, Web Content Filtering, and Messaging Security) has increased significantly since 2002. With annual revenues from SCM vendors growing from US\$4.2 billion in 2004 to US\$7.5 billion in 2008 – a 16% compound annual growth rate (CAGR) from 2003 to 2008.

In addition, based on our FortiGuard Distribution Network, the Fortinet's FortiGuard Web Filtering Service saw a 12.6% increase in Web Filtering Lookup compared to the typical level.

The challenges of keeping users satisfied and safeguarding corporate assets is becoming a daunting task for IT and Security professionals alike. Data security must now evolve into a multi-

faceted approach and be implemented at all aspects of the network - perimeter, DMZ, core, and endpoints. The need to scan, inspect, monitor and control access has become clearer than ever.

TECHNOLOGY FOR WEB CONTENT FILTERING

There are several different technologies that help facilitate web monitoring, logging and filtering of web related traffic. Many solutions are software based and run on Intel based servers that are attached to the network through a "mirrored" network port. Other solutions are dedicated appliances that are installed inline with the network, allowing it to see all of the Internet traffic and allowing it to take fast responsive action against non-authorised and malicious content.

Some of the most common methods for web content filtering include:

- **Banned Word List** – This method allows the creation of a "black list" dictionary that contains words or phrases. URLs and web content is compared against the black list to block unauthorised web sites.

- **URL Block** – The URL Block is a "black list" containing known bad or unauthorised web site URLs. Entire URLs can be added to the black list and exemptions can usually be made to allow portions of the web site through.

- **Category Block** – Category Blocking is the latest web content filtering technology that greatly simplifies the management process of web inspection and content filtering. Category Blocking utilises external services that help keep suspect web sites up-to-date - relying on Web

Category Servers that contain the latest web URL ratings to perform web filtering. Web traffic is inspected against rating databases installed on the Category Servers and the results (good or bad sites) are cached to increase performance. This method ensures accuracy and real-time compliance with the company's Internet Usage Policy.

MULTI-FUNCTION SECURITY APPROACH

The most effective solution to secure an enterprise network is a consolidation of various key security functions that provide a dynamic threat prevention system. Through multi-functional security devices that combine various security features with the ability to receive automated signature and web URL rating updates, the success rate of detecting and blocking new blended threats has increased many times over a single function security device or service.

By sharing information between each component and relying on powerful firewall and IPS capabilities, threats are identified quickly and proactively blocked at the network level before they reach the endpoints to cause damage. Enterprises can create custom Protection Policies by turning on any of the security functions in any combination that is best suited to their specific requirements.

But most importantly, the web content filtering and security solution must offer a wide array of internal and external structured reporting features so that an enterprise can gain a detailed insight into their corporation's internet activities and regain control of their network resources, improve productivity and reduce the substantial risks and legal liability associated with inappropriate and illegal content. **mb-e**