Reference Code: TA001395SEC
Publication Date: April 2008
Author: Andy Kellett and Balachandar Ganesh

Butler Group
a Datamonitor Company

TECHNOLOGY AUDIT

Bloxx Tru-View Technology Web Filter

Bloxx Ltd.

BUTLER GROUP VIEW

ABSTRACT

Bloxx is a provider of third-generation Web Filtering solutions. Its appliance-based Tru-View Technology (TVT) solution is tasked with reducing the risks to business and its users from inappropriate Internet use and as a result helping to enhance employee productivity. Functionally, the company's patent-pending approach to filtering out risky activities utilises all of the conventional components of Web Filtering and then significantly begins its real work by adding layers of analytical intelligence that takes content identification up to a new level. Based on each organisation's usage rules and policy, TVT performs a real-time contextual analysis of each requested Web-page and classifies each access request into pre-defined categories. The solution then makes a rules-based decision on whether to grant or deny access to the requested Web page. Apart from granting controlled access to Web pages, the solution is also able to restrict file and information download capabilities and control the use of Instant Messaging (IM) and Peer-to-Peer (P2P) software. In Butler Group's opinion, TVT brings a new functional perspective to the Web protection marketplace.

KEY FINDINGS

- ✓ The key benefits that TVT provides are based on 'live' Web contextual analysis.
- ✓ Good reporting capabilities enable the use of standard and customised reports.
- ✓ Supports the ability to enable granular, role-based access policies.
- ⓘ TVT is as an appliance based product.
- ✓ The solutions can integrate and interoperate with existing LDAP directory infrastructures.
- ✓ Provides control over common Web usage activities such as IM, P2P, and downloading.
- ✗ Does not currently include an image scanning facility for requested Web pages.
- ⓘ Delivered as a Web-based access management solution.

Key: ✓ Product Strength ✗ Product Weakness ⓘ Point of Information

FUNCTIONALITY

The rapid growth of the Internet over the last few years has been a key business enabler and continues to contribute significantly to the growth and functional efficiency of most organisations. Now, with the emergence of Web 2.0 applications, the dependence of business on the Internet, particularly for communication and collaboration, has grown to such an extent that it would be difficult to fathom operations without the availability of Web-driven services. However, although the importance of operational Web access cannot be discounted, it is well known that social usage at work serves as a source of distraction for employees and misuse of the resource can lead to significant productivity losses as well as posing potential threats to network and information security. Therefore, organisations have a need to implement solutions that enable employees to adhere to acceptable Internet usage policies and at the same time provide the ability to enhance productivity and reduce risk during normal valid Web usage.

Product Analysis

First and second-generation Web filtering techniques have traditionally relied heavily on the use of continuously updated database lists of URLs, which should be blocked and associated white and black listing approaches. However, with literally hundreds of thousands of current unacceptable URLs that have not been identified and with more being added every day, the chances of a bad Web site being accepted as good due to a lack of information is quite high, making reliance on manual database updates to be an inefficient approach unless this forms just the first layer of a multi-layered Web filtering protection approach.

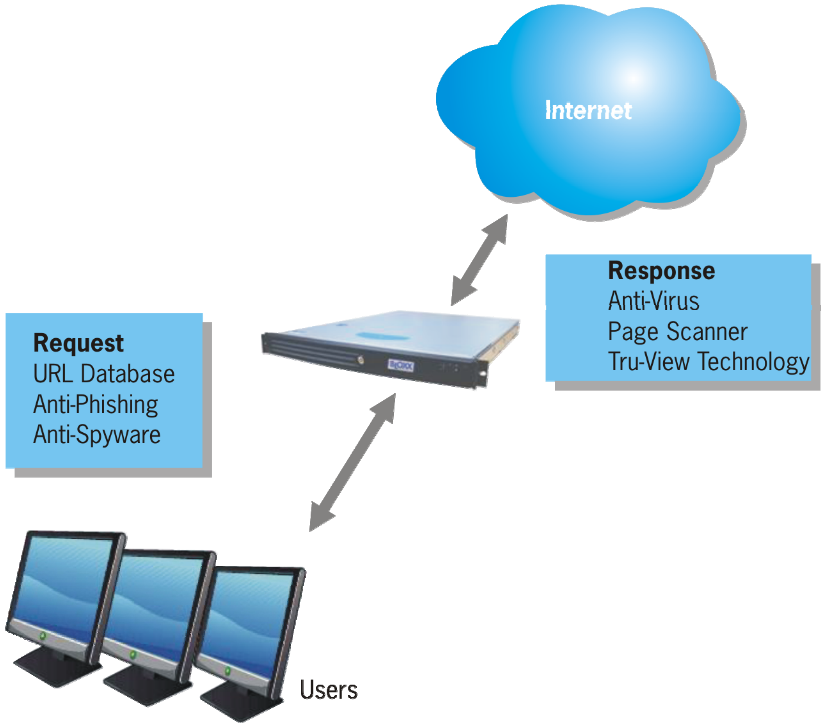
White and black listing and the use of keyword scanning adds to this but collectively all of these component parts still fall short of the levels of business and user protection that are required. For example, bringing the requirement down to a specific organisational level, corporate policy may quite reasonably dictate that users should not be allowed to access Web sites that sell illegal goods or services on-line. Therefore, when using a keyword approach, one of the words that would reasonably need to be scanned for would have to be drugs, but doing this could result in several reliable informative sites falling under the organisation’s unacceptable Internet use policy.

The fact is that the use of URL filtering, keyword scanning, and white and black listing used alone or collectively is no longer effective enough to protect organisations and their users; firstly because a significant number of bad sites continue to be missed, and secondly because such approaches can also fail to accurately classify the content of good Web pages. What is needed is a more comprehensive approach, one that recognises genuinely bad Web requests and rejects them outright, but one that also uses information intelligence alongside the policy and rules of an organisation to make real-time decisions on what Web access requests are and are not allowed.

The Bloxx approach to Web filtering takes into account the value that can be gained from URL, keyword scanning, and listing approaches, and then provides additional layers of analytical intelligence over the top of these first and second generation Web filtering approaches. Basically, within the Bloxx approach, the first line of defence continues to be provided by a database of blocked URLs. If the requested page matches with the list contained in the database, access is denied. If the requested page is not in the list of blocked URLs and it does not appear on a company’s internal blacklists or whitelists, then Bloxx TVT performs real-time contextual analysis of each request and categorises it before granting or denying access to the page.

The Bloxx TVT solution ships with a list of 50 pre-defined categories that would generally meet the filtering requirements of most organisations. Based on these categories and the option to extend these and add others, a definably robust Internet access policy can be put in place for particular users and/or groups of users, with Bloxx TVT taking responsibility for denying or granting Web site access.

Figure 1: Architecture



Source: Bloxx

DATAMONITOR

Apart from blocking Web sites that do not conform to the organisation's acceptable usage policies, the Bloxx TVT solution is capable of controlling access to other forms of potentially unacceptable Web-based activities such as IM, P2P, and unwanted file downloads. Administrators can either block or allow all IM and P2P activity at group and individual levels or can provide specific users and groups with controlled access to acceptable applications. Users can also be prevented from downloading unwanted content especially where size and volume could potentially monopolise network bandwidth and slow down other vital business activities.

The overall Bloxx TVT solution also incorporates the use of complimentary anti-malware facilities through its partner channels where it has OEM agreements on Anti-Phishing, Anti-Spyware, and Anti-Virus protection solutions. Its OEM agreements include Netcraft that provides Anti-Phising scanning capabilities, with basic Anti-Virus capabilities being accessed via ClamAV. Bloxx can also integrate with other Anti-Virus solutions to further address the threats posed by viruses that have increasingly become a cause for concern particularly over the last few years. It maintains a Spyware database, with updates being performed on an overnight basis. Bloxx scans both incoming and outgoing traffic for Spyware and can also be used to prevent other areas of the network from becoming infected.

Product Operation

To provide its operational functionality Bloxx TVT arrives pre-loaded with 50 common Web analysis categories, all of which are listed in Table 1 below. For each Web access request where a clear allow or deny decision cannot be made using traditional Web filtering approaches, TVT carries out contextual analysis of the Web content of the site, and from this places each URL request into one of the aforementioned categories. From here the solution applies the organisation's Internet control policy as it applies to the individual user and makes a decision over whether access is allowed or denied. TVT offers the capability of supporting multiple languages and performing context-based analysis for all languages where scripts are derived from a western European alphabet (for example: French, German, Spanish). The product is capable of working with the text on a Web site, which normally provides adequate information to categorise Web pages, but at this point in time, like all its mainstream competitors, it does not cover image analysis. Bloxx TVT also allows administrators to create additional and extended custom categories and define appropriate rules and policies that pertain to each category.

Table 1: Web Filter Categories

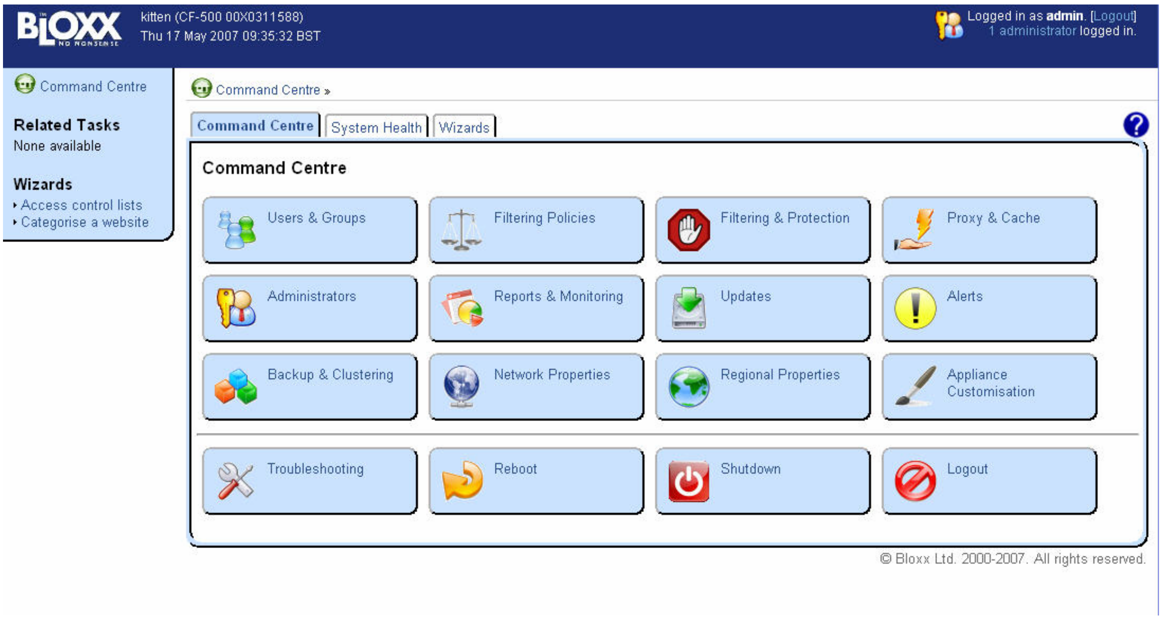
Adverts	Illegal	Religion
Alcohol & Tobacco	Image Sites	Search Engines
Arts & Entertainment	Instant Messaging	Sex Education
Auctions	Internet Telephony	Shopping
Automotive	Lifestyle & Culture	SMS & Mobile Telephony Services
Business & Commercial	Military	Software Download
Computing & Internet	News	Sport
Drugs	Newsgroups & Forums	Streaming Media & Media Downloads
Education	Offensive & Tasteless	Translation
Finance & Investment	Peer to Peer	Travel
Food & Drink	Dating	Violence
Gambling	Pornography & Adult Material	Weapons
Gaming	Property & Real Estate	Web chat
Government	Proxy Avoidance	Web logs & Social Interaction
Hacking	Recreation & Hobbies	Spyware
Hate & Discrimination	Recruitment	Web mail
Health	Reference	

Source: Bloxx DATAMONITOR

The supporting user interface for TVT is, as one would expect, Web-based and is provided by the Bloxx Command Centre (see Figure 2). Command Centre provides the central point of access where administrators go to set up and define all rules and policies that are to be applied against individual users or groups of users. Each set of rules and policies work in conjunction with the contextual analysis performed by TVT in order to ultimately make a decision on whether or not users are granted or denied permission to access each requested Web site.

Rules and policies can be highly customised and can be set according to the organisation's requirements for each individual or user group. For example, organisations may want to block all employees from accessing shopping or social networking sites during normal working hours, but may then be willing to allow access to these specific types of Web site during the lunch period. Rules and processes can be set up using TVT to achieve this and many other variations on the same type of theme. The solution can also be personalised insofar as how users would view a blocked site notification; this could vary from a simple 'site not available' message, through to a more detailed set of rejection reasons which could also be linked to inappropriate usage warnings. Using the Bloxx Command Centre, administrators can also integrate the core functionality of the solution with existing LDAP directory structures.

Figure 2: Screen Shot – Bloxx Command Centre



kitten (CF-500 00X0311588)
Thu 17 May 2007 09:35:32 BST

Logged in as **admin**. [Logout]
1 administrator logged in.

© Bloxx Ltd. 2000-2007. All rights reserved.

Source: Bloxx

DATAMONITOR

Continuing with the policy definition aspect of the solution, one notable feature of TVT is the Sensitivity Manager. Sensitivity Manager allows administrators to define tolerances for each defined category and for each user group within an organisation as they relate to each usage category. For example, the tolerance limits for categories involving sports and news could be set at one level because of the expected benign nature of these categories, while categories for hacking, spyware, and proxy avoidance could have very strict access policies applied. In support of this approach, all policy areas can be considered as continuous work-in-progress areas, they can be refined and built up over time and at the required levels of granularity in line with the needs of the business.

Regular updates to the content of the Bloxx URL database are automatically sent daily on an overnight basis, achieved by the resident user database linking into the host at Bloxx. In addition, customer machines can be used to identify their own bad URLs and these can be passed back to Bloxx who then make further checks before they can be used to form part of the general overnight URL update process to all users.

The solution features a reporting engine which facilitates the generation of standard and customisable reports. Reports of varying levels of granularity can be generated. These are stored within the Command Centre facility and can be integrated with third-party analytics solutions to perform detailed analysis of performance metrics. In addition, when users perform tasks that are outside the boundaries of an organisation's acceptable use policies, real-time notifications or alerts can be automatically sent to authorised personnel so that appropriate actions may be taken.

Product Emphasis

Bloxx TVT provides a third generation Web filtering solution that goes beyond the functional capabilities of traditional first and second generation Web filtering approaches. The solution's decision-making processes to allow or deny user access to requested Web pages are not dependant on any one single dimensional approach. The TVT solution performs a contextual analysis of Web pages that users' request, classifying the pages in real time, and then making an allow or deny decision that is based on the policy of the organisation and the user's own privilege ratings within the organisation.

DEPLOYMENT

Customers choosing to deploy the Bloxx TVT Web Filtering solution can choose to install the appliance themselves or, as appropriate, can have the appliance installed on their behalf by Bloxx engineers. The average installation and configuration time is one to two hours per appliance, with each appliance being shipped with a pre-installed 'fast-start' configuration of default Web access policy facilities.

Training for small-to-medium sized installations is provided on the day of installation. Additional training, if required, is available from Bloxx and can be provided at the customer's site. As one would anticipate, larger installations, that have a need to deploy multiple TVT appliance sets, typically require longer deployment and training times. In this regard, the company works directly with its customers to facilitate large scale installations through its 'Bloxx Professional Implementation Strategy' programme.

For customers that have been supplied with their TVT solution via the company's direct sales channel, customer support is provided directly by the Bloxx technical support staff using phone and e-mail facilities. To support this approach, members of the Bloxx technical staff, can, with the client's permission, directly access TVT appliances for fault correction and troubleshooting purposes. For customers that have made their TVT purchase via the authorised reseller channel, first-level support is provided by the reseller and, where required, problems can be escalated to Bloxx for second-level support.

The Bloxx TVT appliance is Linux-based and, in functional use, it is OS and hardware agnostic. The organisational risk involved in deploying such a solution from a technological standpoint is said to be minimal, with any such risks being more related to user-focused issues relating to employee acceptance of filtering and acceptable use policies, which each organisation needs to continuously review and keep users up-to-date with.

For TVT deployments where the number of supported PCs exceeds 4500, the Bloxx solution is capable of supporting High Availability (HA) and Load Balancing (LB) services. TVT-500 models and above can be configured in clusters of two or more for optimal protection and in support of 'hot swapping' between appliances. TVT-1250 models and above are delivered with raided mirrored drives. Configurations and databases are backed up using a methodology that supports rapid restoration in the event of failure.

PRODUCT STRATEGY

The target market for the Bloxx TVT Web filtering solution has not been defined to have either a specific vertical or horizontal focus as the product is designed to cater for the needs of all network users. To date, most of Bloxx' successful deployments have been into the medium-sized corporate market, to local government and healthcare, and to the education sector. Realistically the company targets its product at any organisation with 50 or more PCs and has a variety of appliances that can meet scalability requirements.

The productivity benefits for solutions of this nature are tangible and can be calculated through the use of simple arithmetic formulae. Although it is typically not clear if the productivity benefits translate to actual cost savings, the number of hours spent on casual browsing and work-time browsing through unproductive content and the total number of employees in the organisation, gives a figure that represents potential cost savings. Tangible benefits are also manifest in the form of reduced risk of Internet abuse and employee harassment, which could result in lawsuits or other legal cases that ultimately lead to financial losses, and the significant reduction in IT management time typically needed with some competitor Web filtering solutions. Furthermore, organisations that have managed to overcome the need to make extended bandwidth purchases following the deployment of the Bloxx solution could position this cost-saving benefit as a real measure of success.

The route to market for Bloxx is both direct and through resellers. The company has technology partnerships with Intel Corporation and Exacta Network Technologies for appliance hardware, and also has partnership arrangements with a number of security vendors whose products can be deployed alongside its Web filter offering to provide additional protection services such as gateway-level Virus and Spyware and Phishing protection.

Product license costs are based on the model of appliance or appliances deployed and not on the number of users. The company has a variety of hardware appliances that are capable of supporting organisations of different sizes, starting with less than 100 users and moving up to support more than 2500 PC users on a single appliance.

In Butler Group's opinion, the Bloxx multi-layered approach to Web protection is well positioned to cater for the needs of organisations with a requirement for policy and rules-based Web filtering that can be tailored to meet the usage demands of differing groups and individuals. Most importantly, while Bloxx continuously updates its database of blocked URLs and these updates are made available to customers on a daily basis, the company does not overly rely on this database as some of its mainstream competitors do. This is a clear differentiator in a market where considerable resources and effort are spent trying to keep such databases as up-to-date as possible. However, we would also point out that the Web filtering sector has witnessed some consolidation in recent times, and other functionally-rich solutions have been acquired by larger players that see this sector of the Web protection market as being of particular importance.

COMPANY PROFILE

Bloxx Ltd. was originally founded in 1999 and is currently being positioned as the fastest growing Web filtering company in what is already a highly-competitive Web filtering security sector. Based in the UK, with its corporate headquarters at Livingston, near Edinburgh, in Scotland and with sales offices in The Hague, Holland, and Boston Massachusetts, US, and Brisbane, Australia, Bloxx remains a privately-held company. During its lifetime Bloxx has received investment funding from leading UK investment groups such as Braveheart Investment Group Plc and Archangel Investments Ltd. This funding has enabled the company to become highly competitive in its market of choice and has resulted in it achieving a position in the top 20 of the Deloitte UK Fast 50 list, and number 76 in the Deloitte EMEA 500 rankings. To date Bloxx has seen around 1000 of its appliances deployed across Europe and its next target is to penetrate the American and Asia-Pacific markets. Amongst its growing customer base the following companies can be considered as reference clients: Graypen; Barking College; JCB; NHS Lothian; Isle of Wight Council; Surrey Satellite Technology; The Diary Farmers of Great Britain; The Money Shop; and Nickelodeon.

SUMMARY

In Butler Group's opinion, the multi-layered protection and contextual analysis approach to Web filtering used by Bloxx in its TVT solution provides a highly-competitive, leading-edge solution in a marketplace that is often driven by vendors whose Web filtering solutions still rely more heavily on the frantic need to keep large URL databases up-to-date. The company's dynamic, customisable, and role-based Web access facilities, coupled with its user-based policies for file downloads, IM, and P2P, rounds off the product's capabilities well. We believe that the Bloxx TVT offering is well placed to continue to serve its core customer base of small-to medium-sized commercial enterprises, government agencies, and education, and is now in a good position to deliver its services into the enterprise marketplace. Overall, an impressive solution that is well-aligned to deal with the dynamic nature of the Internet and current Web usage trends.

Table 1: Contact Details

Bloxx UK
Bloxx Ltd.
Geddes House
Kirkton North
Livingston, EH54 6GU
UK
Tel: +44 (0)1506 426 976
Fax: +44 (0)1506 418 844
E-mail: info@bloxx.com
www.bloxx.com

Bloxx Inc. – USA
Bloxx Inc
113 Terrace Hall Avenue
Burlington
Massachusetts 01803
USA
Tel: +1 781 229 0980
Fax: +1 781 998 0540
E-mail: info@bloxx.com
www.bloxx.com

Bloxx Europe
PO BOX 10537
2501 HM
Den Haag
Netherlands
Tel: +31 (0)70 320 5009
Fax: +31 (0)70 320 1105
Email: info@bloxx-europe.com

Bloxx Australia
12-14 Marine Parade,
Southport
QLD 4215
Tel: +61 1800 225 699
E-mail: info@bloxx.com
www.bloxx.com.au

Source: Bloxx

DATAMONITOR

Headquarters
Europa House,
184 Ferensway,
Hull, East Yorkshire,
HU1 3UT, UK
Tel: +44 (0)1482 586149
Fax: +44 (0)1482 323577

Butler Direct Pty Ltd.
Level 46, Citigroup Building,
2 Park Street, Sydney,
NSW, 2000,
Australia
Tel: + 61 (02) 8705 6960
Fax: + 61 (02) 8705 6961

Butler Group
245 Fifth Avenue,
4th Floor, New York,
NY 10016,
USA
Tel: +1 212 652 5302
Fax: +1 212 202 4684

For more information on Butler Group's Subscription Services please contact one of the local offices above.

Important Notice

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.