Internet Monitoring Software For University Health Systems Of Eastern North Carolina

Gordon Giles

Course: DTEC 6823
Professor: Dr. Lunsford
Date: November, 2005
Abstract: The emergence of technology over the past 10 years has forced organizations to take a long hard look at the productivity levels of their employees’. The Internet has become such an integral part of business practices that many companies would not survive without access to it. This powerful tool that our organizations rely on so heavily can also have a negative impact if abused. If some type of monitoring tool is not put into place these companies stand to lose hundreds if not thousands of dollars due to employee negligence. By simply putting into place a software package and configuring it to match your Internet Acceptable Usage Policy will save your valuable employee resources from inappropriate Internet use. Due to reports of inappropriate Internet use the Executive staff of the University Health Systems has made a decision to install an Internet Monitoring Tool to prevent employees’ from abusing the Internet Usage Policy. The choice for the software platform has been narrowed down to 3 of the top Internet filtering software companies on the market. Websense Inc., SurfControl Inc., and St Bernard’s Iprism are the companies that have been selected for evaluation. It has been determined that filtering inappropriate sites is more of a concern than trying to report on individual abusers, in other words if a user cannot access an inappropriate site then there should not be a reason to run a report on that user. The company that can prove to be strong in filtering URL categories, policies, and to some extent reporting will be awarded the contract. The following document is the official Internet Usage Policy of University Health Systems of Eastern North Carolina, which is the basis for the following research.
I. General Background

The Internet is a term which is used to express the world wide connection of computers and networks. There are now a number of powerful tools which can assist you at your job. Internet mail may be used to improve communications with colleagues. While Netscape can provide you with access to the World Wide Web for information about products and services. With all of this accessibility, comes responsibility.

Below we have outlined appropriate use of the Internet:

II. Permitted Internet Use

A. For acquiring, distributing, or exchanging Information of administrative, medical, scientific, or technical nature which supports PCMH business and research.

B. For approved education which supports PCMH or its employees.

C. For an activity which contributes to the mission of PCMH.

D. For other purpose approved by management.

III. Prohibited Internet Use

A. For any activity which violates PCMH, State of North Carolina, Federal Government, or other Nations, rules and/or laws.

B. For any activity which could cause harm to PCMH, from a Business, Economical, Legal or Image standpoint.

C. For any activity which transfers Confidential, Vital or Proprietary information, either PCMH maintained or maintained by any other organization.

D. For unauthorized uses of any: Network, Server, or Computer, whether they belong to PCMH or any other organization.

E. For any unapproved activity which uses large bandwidth or computational requirements, such as real time video, or sound programs.

F. For any activity or distribution which disrupts PCMH, or any other organization's Resources, such as chain letters, computer viruses, computer worms, games, or other leisure software.

G. For any Solicitation for one's personal business.
IV. Network Security

Being on the Internet also comes with more hazards, and We All need to be actively aware of the following:

A. Our passwords should be secure and not easy to guess.

B. Downloaded files may contain Viruses.

C. Use of non-approved applications may open up your machine to unauthorized access.

D. Unknown E-mail may contain destructive viruses.

E. User data should be routinely backed-up.

V. Information Systems Policy

A. IS will provide the user with as secure an environment as possible.

B. IS reserves the right to monitor and log any Internet connections.

C. IS reserves the right to take appropriate action against any individual who does not comply with the outlined responsibilities.

VI. Summary

Internet access is offered as a service to PCMH employees as a tool for communication and research. Each employee must do his/her part to keep PCMH resources secure by following the outlined security guidelines. If you have any questions concerning the Internet and its use please let us know at 816-5111.
Websense Inc. is a California based software company that specializes in Internet filtering software for more than 20,000 companies worldwide [9]. Websense is currently ranked 11th on the FSB 100 list of companies and they employ 388 with Mr. John B. Carrington serving as CEO [9]. The company provides an enterprise solution for monitoring employee Internet usage and also analyzes bandwidth and storage use on their clients’ networks with a proprietary database of at least 1 billion web pages spanning over 90 categories [9]. Websense integrates very well with the following firewall software companies, Cisco Secure Pix Firewall, Checkpoint Firewall-1, Microsoft Internet Security and Acceleration Proxy Server, and the Cisco Cache, Engine [6]. A reporting tool is also incorporated into the product using an SQL or MSDE data engine for printing or e-mailing individual reports to interested parties [5]. Websense goes beyond basic filtering with features such as the basic time quota that allows administrators to control the amount of time a user can surf the Web [13]. Websense is very easy to install and implement and also does everything that the company advertises as well as giving administrators a break on having to track down and confront employee’s with reports of inappropriate surfing [13]. There are 2 types of Internet filtering techniques, the first method examines the web page in real time and algorithmically examines the data dynamically determining the content, the second method uses a database with predetermined site information that has been categorized by humans [22]. The database approach has proven to be 100% accurate in blocking unwanted websites as long as the database is managed appropriately while the dynamic filtering solution often blocks sites that are supposed to be allowed creating over blocking [22]. Websense uses the database method which allows for more categories with higher precision, minimizes false positives, handles media other than just text, and also is harder to fool than a dynamic filtering tool [22]. Websense also offers additional add-on Premium Groups that can be purchased along with the
Enterprise software that allows for extended blocking capabilities, Premium Group I consists of the following categories-

- advertisements
- message boards & clubs
- freeware/software downloads
- online brokerage & trading
- instant messaging
- pay-to-surf ”

Premium Group II consists of the following categories-

- Internet radio & TV
- personal network storage/back-up
- Internet telephony
- streaming media
- peer-to-peer file sharing ”

Premium Group III which is the security package includes these additional categories-

- sites infected with MMC
- sites that implement spyware applications
- scans for MMC on your company's Web site with Websense SiteWatcher ”

Some disadvantages are that Websense occasionally blocks websites that should not be considered offensive such as “The Liza Minnelli Web Site and Jewish Teens page” to name a few [19]. Websense has also been sited to have some security flaws allowing a remote user to access authentication cookies associated with the site that is running the Websense software and
could possibly allow them access to sensitive data [17]. Another down side for Websense is that it requires 3 pieces of hardware, one for the server application, one for the log server, and another for the reporting tool which brings the cost up significantly [9].

**Case Study:**

Tempe-based Avnet Enterprise Solutions has signed an agreement to partner with Websense Inc. “As an extension of its security solutions, Avnet Enterprise Solutions now will provide enterprise customers across the nation with Websense solutions, complete with assessment consulting and implementation services unique to the employee Internet management (EIM) market. In addition, with Websense Explorer, Avnet Enterprise Solutions enables corporate managers to click through employee Internet use information in order to analyze trends and identify high risk Internet use, such as hacking, malicious code and Internet storage applications. Avnet Enterprise Solutions is a solutions integrator specializing in enterprise server, storage and network solutions that power business applications. The company is a subsidiary of Phoenix-based Avnet Inc., a technology marketing, distribution and services company” [18].

SurfControl is another California based company that ranks among the top for Internet filtering worldwide with 20,000 customers and 450 employees’ with Stephen Purdham serving as CEO while the company is spread out over 9 locations across the United States, Europe, and Asia [3]. Listed are some of the SurfControl features that are included to make it a complete solution, e-mail (Spam) filter of SMTP, e-mail (Spam) filter for exchange, web filters for windows, web filter for ISA, and instant message filter [3]. SurfControl partners with some of the largest companies within the industry such as Cisco, IBM, CheckPoint, and Microsoft [14]. SurfControl works much like Websense in the sense that it is very scalable and fits into any
environment no matter what size network you install it into and it also uses a large database that classifies websites into a category set of 40 entries [16]. It also uses rule criteria in which bandwidth allocation and employee usage time parameters can be configured to company specifications [16]. Dynamic filtering can be used with an optional plug-in component purchased separately that works using “neural network technology” and will identify future questionable sites that have not been classified to date [16]. A total of 55 reports can be generated ranging from Internet usage reports and reports indicating trends that will help reduce traffic and excessive on-line activity [16]. SurfControl makes three points as to the reason some type of internet monitoring is necessary, it helps to manage inappropriate Internet usage by employees’, it filters bandwidth usage from sites such as Kazza and Napster, and it prevents potential lawsuits from resulting due to sexual harassment claims from inappropriate surfing behavior [4]. SurfControl introduced their complete line of products to the International Content Certification Standards board and was awarded the ICCS certification along with being recognized by the United Federation of ChildSafe Websites (UFCWS) [7]. SurfControl has many advantages such as the Virtual Learning Agent that acts like an intrusion detection agent protecting confidential company information [2]. A strong selling point for SurfControl is the fact that it can be purchased as a complete integrated package with web filtering and E-mail filtering which includes the prevention of such programs as spyware, gator, and other malicious software from infiltrating the customers network [1]. Another strong advantage is that SurfControl is very prevalent in the school systems around the country and is showing up in more and more homes [1]. SurfControl also has some disadvantages such as a known problem with database updating so a large portion of classifications will be omitted and the report monitoring analysis tool is useful when it’s working but is difficult to set up [4].
A bug has also been identified that allows remote users to arbitrarily gain control of files on a Microsoft ISA server running the SurfControl software [4]. The growth of the Web has made available anything an employee could possibly need at their fingertips, but not all are gathering vital business information and emailing important clients. “There are few modern businesses that could survive without the Web: an indispensable source of information on any subject, and the most rapid and effective form of correspondence. Unfortunately, Internet connectivity also creates a host of temptations.” SurfControl conducted a recent survey that showed 60% of employees' Internet activity includes visits to non-business related sites. This type of activity can be avoided with the proper controls in place [15].

St. Bernard Software Inc. is yet another California based company but has a different type of product on the market called Iprism [10]. The company started with 12 employees in 1995 with one product and today generates more than 200 new customers per month with 4 products, Open File Manager, UpdateEXPERT, iPrism, and ePrism with Mr. John E. Jones serving as CEO [10]. The focus of this research will concentrate on the iPrism solution, which has become the product of choice for Internet Access Management to help enforce the Internet Usage Policy within organizations. This cost effective Internet monitoring appliance has been recognized as winning the highly coveted P.C. magazine’s “Editor of Choice Awards [10]. The appliance has a Pentium-based processor with 128 megabytes of memory using Unix utilities and Java for console administration [6]. The software uses a central repository of over 60 categories of filterable content and is updated nightly from St. Bernard headquarters and they also guarantee that all categories are inspected by human eyes [10]. IPrism integrates very well with the following firewall companies, Cisco, CheckPoint, Microsoft, IBM, and improves
network response time by conserving bandwidth by controlling employee usage to Internet access [11]. Some of the key features that the iPrism appliance has are listed below.


**Case Study:**

Lodi Memorial Hospital is a non-profit, acute-care hospital, owned by the Lodi Memorial Hospital Association. They presently have a network of seven servers and 600 workstations at four locations. “Lodi Memorial Hospital's IT staff faced a monumental challenge when one of the hospital's key employees was discovered accessing highly inappropriate Internet sites on a regular basis. After dismissing the staff member, the hospital's director and board called for quick action to prevent subsequent Internet abuse.” After a consultation with Alliance Computer Technologies they recommended St. Bernard's iPrism appliance. After one week of implementation, Lodi's IT staff were convinced that the appliance approach provided by iPrism was the best solution. St. Bernard Software's iPrism is a self-contained appliance that filters by full URL name and includes the ability to block top-level directories while allowing access to subdirectories. Its database is 100% human-reviewed, and includes millions of sites over 60 different categories. This database is updated daily with thousands of new sites. Companies can add their own categories and URLs to this list or create "white lists" of trusted sites. Lodi experienced low initial cost, ongoing savings, ease of use for users, and the ability to run reports [20].
Conclusion: All three of these products would be an excellent fit for the Internet Filtering Tool needed on the UHS East network for monitoring and filtering Internet traffic. SurfControl integrates very well with all the firewall products and is very attractive with the inclusion of the e-mail filtering tool. PCMH and its subsidiaries already have in place an e-mail filtering software package so unfortunately would not be able to take advantage of this feature. I feel like the price of SurfControl with the added hardware that is required to run the database is a little bit more than the hospital will want to budget for. Although a very good product I would have to eliminate SurfControl due to the expense. Websense seems to have the best database software on the market. Websense also integrates very well with Cisco firewalls, which is a perfect match for UHS East. The reporting log server is also a very attractive feature producing numerous reports for management. Unfortunately Websense also requires three extra pieces of hardware that increases the price of the product substantially and with the high quote given by their representative puts Websense out our price range. My recommendation for the UHS East Internet Filtering Tool is St. Bernard’s iPrism appliance. This product beats both competitors hands down in my opinion. There is no additional hardware needed and the price is more than a $10,000 difference from the other two products. The appliance integrates with less network resources and seems to be a better fit with a Cisco Pix firewall than Websense or SurfControl. The database and reporting tool seem to be comparable with the other products but the Unix based operating system and the Java enabled console are more appealing than the Windows based platform that Websense and SurfContol use. I believe that iPrism is an excellent choice for the Internet Filtering Tool for University Health Systems of Eastern North Carolina. The next
The document shows a comparison of all three products, which clearly shows iPrism to be the best choice available.

**Comparison Chart, for several industry-leading product lines...**

<table>
<thead>
<tr>
<th></th>
<th>DynaComm</th>
<th>i:filter</th>
<th>iPrism</th>
<th>SurfControl</th>
<th>Websense</th>
<th>X-Stop R2000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Details</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pass-BY Mode</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>currently under review</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Pass-THRU Mode</strong></td>
<td>No</td>
<td>Yes</td>
<td>currently under review</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td><strong>Comprehensive Blocking</strong></td>
<td>Yes**</td>
<td>Yes**</td>
<td>currently under review</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Available Formats</strong></td>
<td>Software-only</td>
<td>Appliance</td>
<td>currently under review</td>
<td>Software-only</td>
<td>Appliance and Software-only</td>
<td></td>
</tr>
<tr>
<td><strong>Database Quality</strong></td>
<td>Excellent</td>
<td>Excellent</td>
<td>currently under review</td>
<td>Excellent</td>
<td>Excellent</td>
<td></td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>Platform Dependent</td>
<td>Excellent</td>
<td>currently under review</td>
<td>Platform Dependent</td>
<td>Excellent</td>
<td></td>
</tr>
<tr>
<td><strong>Reliability</strong></td>
<td>Platform Dependent</td>
<td>Excellent</td>
<td>currently under review</td>
<td>Platform Dependent</td>
<td>Excellent</td>
<td></td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td>Excellent</td>
<td>Excellent</td>
<td>currently under review</td>
<td>Excellent</td>
<td>Excellent</td>
<td></td>
</tr>
<tr>
<td><strong>Ease of Use</strong></td>
<td>OK</td>
<td>OK</td>
<td>currently under review</td>
<td>OK</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td>Very Good</td>
<td>Very Good</td>
<td>currently under review</td>
<td>Excellent</td>
<td>Excellent***</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Yes</td>
<td>Yes</td>
<td>Currently Under Review</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------</td>
<td>--------------</td>
<td>------------------------</td>
<td>--------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>Logging vs Blocking</td>
<td>Yes</td>
<td>Yes</td>
<td>Currently Under Review</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Reboot Time</td>
<td>Platform Dependent</td>
<td>Short</td>
<td>Currently Under Review</td>
<td>Platform Dependent</td>
<td>Long</td>
<td></td>
</tr>
<tr>
<td>User Messaging</td>
<td>Yes</td>
<td>Yes</td>
<td>Currently Under Review</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Currently Under Review</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
References

[1] CE of Surfcontrol comments on growing need for Internet filtering software.

[2] Corbelli Martino. How Internet and E-mail misuse in the Workplace Can Damage Your
    Business Sovereign Publications Limited. Retrieved from

[3] Davinsi Products (n.d.) SurfControl: the World's Number 1 Web and E-mail Filtering


    Retrieved from http://www.pcmag.com/article2/0,1759,15048,00.asp.


Database and Network Journal, August, 2002


2003 American City Business Journals Inc.


at Lodi Memorial Hospital

http://www.group1iam.com/pxws.html.