Proxy Servers

PROBLEMS THEY SOLVE AND CAUSE

Group 12

Hamdija Čustović

Eric Gaddy

Asad Khan

Yugi Luu

Introduction

Think about a checking out a book from the library's locked floors, how does one get these books? A library worker is needed that has a key, goes to the locked floor of the library and retrieves the book. What if each time a different book is received the library clerk made copies of the book(s) and puts on a shelf for frequently used books? This copying and indexing would decrease the wait time for someone to get a book. No longer does one have to wait for the clerk to go up to the tenth floor, get the book and bring it back. This would also aide the library by having only the clerk go to the locked floor, not only that, clerks would not have to go the locked floor near as often.

This analogy is that like a proxy server. A request for a webpage (the book) is made; the proxy server (the library clerk) receives the request, goes to the web server (the locked floor) and retrieves the book. The webpage is then brought back and copies are made for others use access more quickly. By the end of this report, the reader will gain an understanding of the following:

- What proxy servers are
- How they work
- Different types of proxy servers
- Common uses
- Problems they solve
- Problems they cause
- How to set up a network using a proxy

Methods

The main methods of research on the topic of proxy servers were searches of the electronic journal and article database provided by EBSCOhost as well as searches of articles and reports on the internet using search engines such as Google. In addition, hands on research was used to obtain information on how to set up networks using proxy

servers and what benefits and problems were observed. EBSCOhost was used extensively due to the current wide use of proxy servers. There were numerous articles of experiences with proxy servers from reputable companies like ABN AMRO, the banking giant and computer magazines such as ComputerWorld. 'Proxy Servers,' 'proxy firewalls,' and 'proxy benefits' were all search strings used on EBSCOhost. The information found using EBSCOhost was useful in the *Discussion* section of the report. Google helped provide information of internet articles and reports from sources such as 'Network Magazine' as well as case study reports from public and private universities. Search strings such as 'proxy servers', 'proxy servers what they are', 'proxy server problems', and 'proxy servers how they work'. These were most useful in the 'Findings' section of the report.

Findings

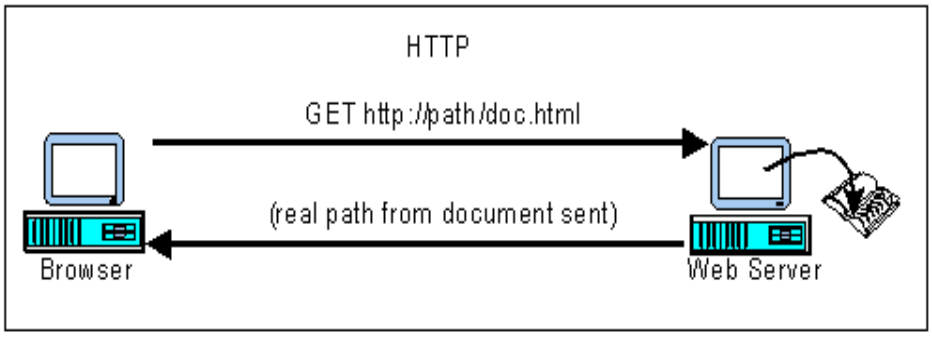
What they Are

Proxy Servers are software that act as intermediaries between client and servers on the Internet. They help users on private networks get information on the Internet when they need it while maintaining network security. They also store frequently requested information such as webpages, in cached memory for faster delivery in the future to multiple users, thus improving download speeds.

How they Work

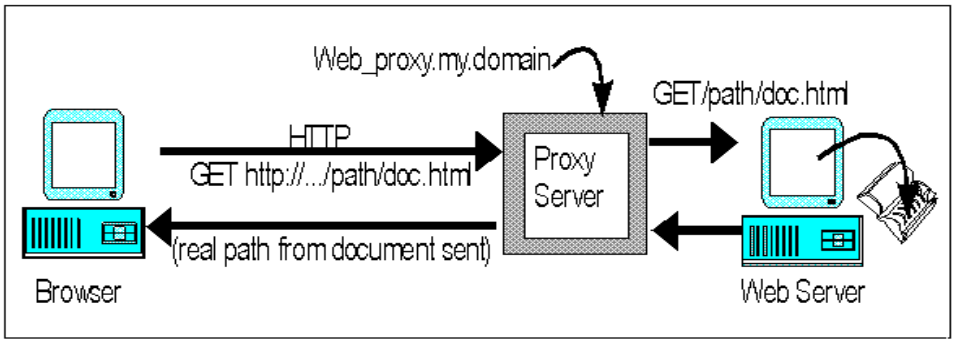
In a normal proxy-less web transaction, the user (client) would use something like a browser to make a webpage request from a web server (See Figure 1 [12]). The network routers and switches would move the transaction request until it gets to the destination (web server). Along with the transaction request, the web server also receives information about the sender such as the IP addresses and uses the address to send back the requested webpage. [1]

Figure 1



In a web transaction that uses a proxy server the transaction would occur differently (See Figure 2 [12]). Instead of sending the webpage request directly to the web server, the user (client) would send the request to the proxy server as directed by the browser configuration. The network routers and switches would move the requested data to the proxy server. The proxy server would strip packets of the client's IP address in order to provide anonymity. Next, the proxy server would send the request to the web server using routers and switches to transfer the request to the web server. In case the web server does not allow for hidden IP address, the request would be denied. Normally the web server would grant the request and send the webpage to the proxy server. The proxy server would check the webpage and filter according to its configuration. Static webpages would temporarily be stored in cached memory for faster access in the future. Thus, the next time the user requests the same webpage, the proxy server would no longer have to send the request to the web server. Instead it would just send the webpage to the user, thus making the whole process faster and conserving the bandwidth. [1]

Figure 2



Types of Proxies

There are two main types of proxy servers, mechanical and application proxies. These differ in the way the client's computer is configured. Proxy servers can further be specialized to meet the needs of the user. They can be specified to handle only certain types of protocols such as HTTP and FTP. They can also have additional complimentary software to enhance functionality and configurability. The main advantage of proxy servers is that they allow a user to gain access to a website from an off campus* location, as shown in Figure 3. [12] This off campus location means outside of the corporate office LAN.

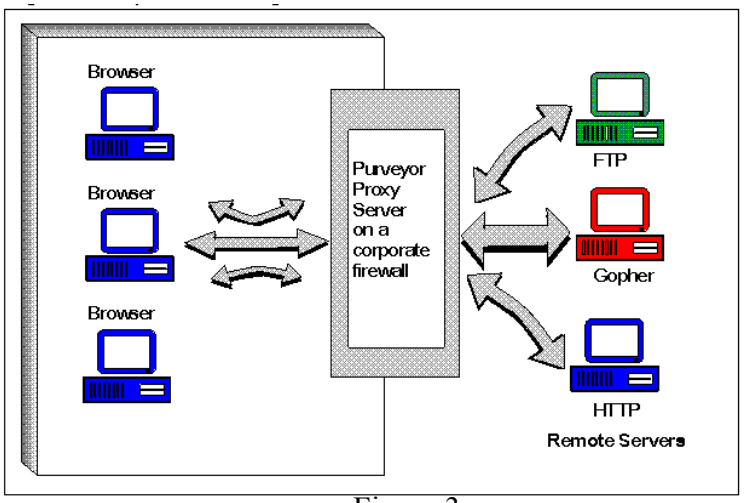


Figure 3

Mechanical Proxy Servers

Mechanical proxy servers require the user to configure their web browsers to the Internet address of the proxy server. The user must also configure which website they wish to be routed by the proxy server. The mechanical proxy servers are compatible with virtually all web browsers such as Netscape and Microsoft Internet Explorer, with the exception of AOL web browser. After the proxy server has been configured correctly, the process it performs is not able to be seen by users and content providers. [2]

Application Proxy

The second type of proxy server is the application proxy server which works much like a mechanical proxy server with one major difference. Like the mechanical proxy server the application proxy server sits between users and the desired websites, but they do this by actively rewriting web addresses on a local proxy. This enables the end

user's workstation to never interact with the desired web site. No configuration of the user's web browser is required, unlike the mechanical proxy servers. A user is required to code in the provider's web page, which sometimes causes the proxy to malfunction. [2]

* Campus is used to represent a local area network, such as an office building or a university.

Additional Features of Proxy Servers:

Firewall Proxies:

While regular proxies provide protection on the application level, the firewall proxies also provide protection on the network level of the OSI model. A firewall proxy reassembles an entire stream of data in order to detect and also remove potentially dangerous attachments before they enter the network. Also, the firewall proxy examines the payload of all data packets running between the server and client. This allows the firewall proxy to modify or delete data packets that violate network security policies. Proxy firewalls are different from packet filters because proxy firewalls examine the entire packet's content, when the packet filters only examine packet headers. Proxy firewalls can make the network safer by making the network extremely difficult to hack by blocking entire categories of commonly used attacks. Furthermore, firewall proxies have the capability of improving bandwidth by preventing unwanted requests from entering the network. Use of firewall proxies helps make network management easier by allowing administrator tools to be applied on a broad basis rather than having to apply them individually for every computer.[3]

HTTP Proxy:

HTTP proxies are used for monitoring web traffic. The standard port amongst web servers for receiving traffic is port 80. Most Web servers receive their traffic from port 80. HTTP proxies block any incoming web traffic that attempts to enter the network in unanticipated ways. Certain websites contain programs that use java and active-x controls. These programs could do unwanted actions from something simple such as setting the home page, to more dangerous interference. HTTP proxies are used to block Java and ActiveX applications. Also, it is the HTTP proxies that are used by

corporations to prevent employees from visiting offensive or otherwise unwanted sites from the company network. [3]

FTP Proxy:

Just like the HTTP proxy filters incoming and outgoing traffic coming via the World Wide Web, the FTP proxy controls FTP traffic sent by the FTP server. It handles the transmissions of large files. Since, FTP servers are susceptible to unwanted requests and attacks, the FTP proxy controls these threats by limiting the number and type of FTP commands that a user is allowed to send FTP proxies. FTP proxies can also be used to specify whether or not files can be downloaded or designated as "read only". They can also set a time limit on connection so that it can disconnect from idle or hung connections.[3]

Problems They Solve

Security

Security is one of the two main problems that proxies help solve. Proxy servers provide security by filtering requests, both incoming and outgoing, on a connection such as the internet. They determine what will be allowed for transmission, reception, or access. Proxies can be used to keep users out of visiting particular websites based on URL addresses or to prevent others from gaining access via IP address authentication. In addition, proxies can scan data for viruses or inappropriate words. Companies can take advantage of proxy servers to prevent employees from accessing specific websites. [4] Even though firewalls can be used to filter any incoming requests on the network layer, they cannot avoid being "attacked." Since proxies operate on the application level, they can solve the problem by breaking any direct link between client and server and simply look at an IP address to determine whether to allow connection. In addition proxy servers have great capability for configuration at the application layer. Proxies can be used to limit applications to deal with only certain types of files.[5]

Conserve Bandwidth

Secondly, proxies have capability to improve performance, also known as proxy

caching. As they scan data, proxies can determine which data should be stored in cached memory so that they can later be used for immediate access. In this manner, typical requests such as websites do not have to be made to the web server every time. Instead, one time is enough for the proxy server to provide temporary storage. This is useful for visiting websites that do not change very often. Proxies are also useful in setting up local area networks to share internet connection. [6] (publicproxyserver.com)

Problems they Cause

Availability of Software

Even though proxy servers offer many benefits to business managers and individuals to safeguard their privacy and restrict unwanted access to the Internet, it comes with some drawbacks. First is the scarce availability of software for the proxy servers to address such Internet services as Real Audio. The rapid introduction of new services is such that the creation of proxy software to support these services is lagging behind in its application. [7]

Limited Virus Protection

The next problem concerns security. While the popularity of proxy servers is based on its ability to keep protocol operations safe, this isn't always possible especially concerning the dreaded virus as a flaw, proxy servers can not differentiate between ordinary emails and viruses sent online. If a user does not have virus scanner plug-in on the proxy and downloads an infected email, the proxy will not be able to detect the virus which could cause an entire network to become infected. Once inside, the proxy server is basically useless as far as stopping this security breach. [8]

Anonymity Abuse

Proxies normally act as gateways between local users and remote sites. What is not always apparent is that they can also be used by remote users to access remote sites. This is usually done by those users who are doing something illegal and want to conceal the origin of network misuse. Whoever owns the proxy can be made to appear responsible for those activities when in fact they're not. Those proxies that are accessible

by remote users are often termed "open proxies" and the list of them is available to them. The only way to combat this problem is to only allow connections when IP addresses can be detected. These restrictions can be expressed using access control lists which permit or deny access based on IP addresses.[9] Even though this security feature may seem like a problem solved for some, for others it can only translate into a different problem.

Limited Access

The ability of proxy servers to provide a secure environment is a major advantage and an asset. However, sometimes this advantage can work against the user depending on what he/she wants to do. For example, if a user wants to gain access to a database website, most of these types of websites require IP detection which is otherwise not favorable for the user, but in this case it is necessary for detection of access (authentication). If the user's proxy server does not allow for IP detection from an outside server making requests, he/she will not be able to gain access to the database website. Also, some proxies interfere with placement of cookies which may cause problems in browsing certain websites.[10]

Configurability

Proxy servers, like firewalls, protect a network from unauthorized access over the Internet. Conversely, often the user wants certain traffic or requests to come in, while preventing others. Firewalls use packet-filtering mechanisms and can be configured using a set of rules that define the actions to be taken. Proxy servers are not as configurable. This is because proxy servers are based on application-level gateway and thus rely on application code to perform traffic filtering. [11]

Another problem is the need for multiple proxy servers for each separate Internet service which include FTP, HTTP, Telnet, Gopher, and WAIS. As with the lag time between proxy servers covering a new service tracking down a server to cover each Internet Service may take considerable time if some proxy servers have not been developed and implemented yet. There's also the time spent installing each separate sever and coordinating each server to its own protocol.

Compatibility

Additional problems may occur with use of certain browsers that cannot be configured to use proxy servers, such as AOL. Furthermore, proxies are bottleneck of network access, if it is down, the whole intranet is down. These problems may be solved by using a different browser or by setting up a redundant proxy server.

Discussion

Business Uses

To a company manager, the productive use of company resources is paramount. For example, while most employees diligently do their job to the best of their abilities with the resources provided, some will attempt to use the same recourses for selfish reasons such as surfing the web for entertainment purposes like visiting adult web sites, online gambling, interoffice chatter, sending or receiving personal emails, and personal online stock trading. This can lead to a serious loss in productivity and lowering of employee moral. Many managers now see the benefits of implementing the proxy server which filters requests by employees to deny access to a specific set of websites.

Data theft is a constant worry for managers and individuals who value their privacy. Annually, online thieves purloin an estimated $10 billion worth of data. Much of this theft comes from business files and individuals' financial information. Most companies have begun using proxy servers which are attached to a firewall host which monitors user requests for Internet access on systems such as FTP, HTTP, Telnet, Gopher, and WAIS. These requests are either forwarded or denied according to the security policy set up on the site. This limits incoming unwanted requests for data from the company's site or files.

A small scale example of using a proxy server would be similar to the one used in the hands on research section below. Perhaps someone uses a cable modem service such as Road Runner™ or DSL (ADSL) such as BellSouth™ DSL service wants to share the connection with others. Generally the shared users would be in the same dwelling or

nearby such as an upstairs/downstairs apartment. There are a few choices here; if the goal is simply to offer simple Internet services such as webpage browsing, ftp, and email then a simple connection of the clients to a hub and configuration of their computers to connect through a proxy server that is installed on a central computer. On the other hand, an Internet connection could be shared through a router which *routes* the computers to the Wide Area Network (WAN). If the latter of the two is chosen, and wish to conserve bandwidth, since it is limited generally to less than two megabits per second (2Mbps), you could configure your clients to connect through a proxy server sitting on your computer. The server would, as explained later, store already visited web pages and can be configured to filter out certain types of content or specified sites altogether. This would be extremely beneficial if the "clients" were children.

Universities, High Schools, and any other educational facility with access to the Internet would use a proxy server. As always, one reason would be to conserve bandwidth. Next and foremost for children and teens would be filtering the content. There are a couple of options a school can choose. You can install a local proxy server and have someone maintain it and update the content to filter or you can get "a "proxy" server filtering program which is a server maintained by an outside off-site service that acts as a liaison between the user and the Internet."[13] Services such as Surfwatch Educational Edition 3.0, Cyber Patrol, K-12World CyberLibrary, and Safe Harbor to name a few are options for schools or anyone for that matter who wish to filter unwanted content.

Hands-on Research

For hands on research, a WinGate proxy server from deerfield.com was installed on a network with five computers. (See Appendix 1) The WinGate software was application based primarily. If preferred, the browser can be configured manually. The network was based on a cable connection and routed through a Linksys router and switch. The proxy server was installed on a main computer (Computer 1) and different tests were run. Test one consisted of using the downloaded application to manage the proxying.

The router was configured to stop WAN connection to all computers but Computer 1. Client software was installed on the four other computers and handled the proxy connection automatically. Internet Explorer was able to connect to the proxy and allowed the client computers to access web pages via the proxy. Applications such as AOL Instant Messenger™, WeatherBug™, IRC, and other non standard port applications caused a problem. Only WeatherBug was able to connect to the Internet with some persuasion. Test two consisted of manually configuring the Browser and other applications to access the Net. With this configuration, only Internet Explorer was allowed to connect.

The most effective of the tests, number three proved to be the most fun. With the still manually configured web browsers, the router was configured to allow Internet access to computers two through five. Port 80 requests were then handled by the proxy server and all other applications used a direct connection through the Linksys router. With permission from the client users, who happen to be my roommates, content and sites were monitored from Computer 1's server. As imaginable, the content of sites viewed by these clients could be questionable if visited in a corporation setting. This led to the installation of a plug-in for WinGate. GateFilter was added and set to a conservative blocking status. To obtain a trail copy of WinGate Proxy Server, go to http://www.deerfield.com/products/wingate/.

The uses for Filtering are evident in a corporate setting. As Marguerite Reardon said, "Sex sells, no matter the medium. Sex also slows, at least on the Web."[14] No one wants his employees wasting valuable bandwidth with smut, nor do they want the possible pending lawsuit on their hands.

Conclusion

As in the library example, proxy servers can make retrieval of information faster and more convenient. Additionally, they provide network security and help control access. Proxy servers are more than useful for large local area networks where there are

multiple users using the same internet connection. They also help businesses manage employee activities on the internet and maximize productivity.

Executive Summary

As the Internet grows, users are looking for more efficient ways to retrieve webpages and control access to websites. Proxy servers are software that serve as intermediaries between users and servers. In a proxy web transaction, the users make requests from the proxy servers instead of the web servers. The proxy servers filter the requests, provide anonymity for the user, and retrieve the webpages for them. Once those webpages are retrieved, they are stored in cached memory for quicker retrieval afterward.

There are two main types of proxies: mechanical proxy servers, and application proxy servers. With mechanical proxy servers, the user has to configure the computer for the use of proxy server. On the other hand, with application proxy servers, the application software does automatic configuration of the computer for the use of a proxy server. Additional features of proxies are firewall proxies, HTTP proxies, and FTP proxies. Firewall proxies help provide additional network security. HTTP proxies are used for monitoring web traffic while the FTP proxies are used for controlling traffic sent by the FTP server.

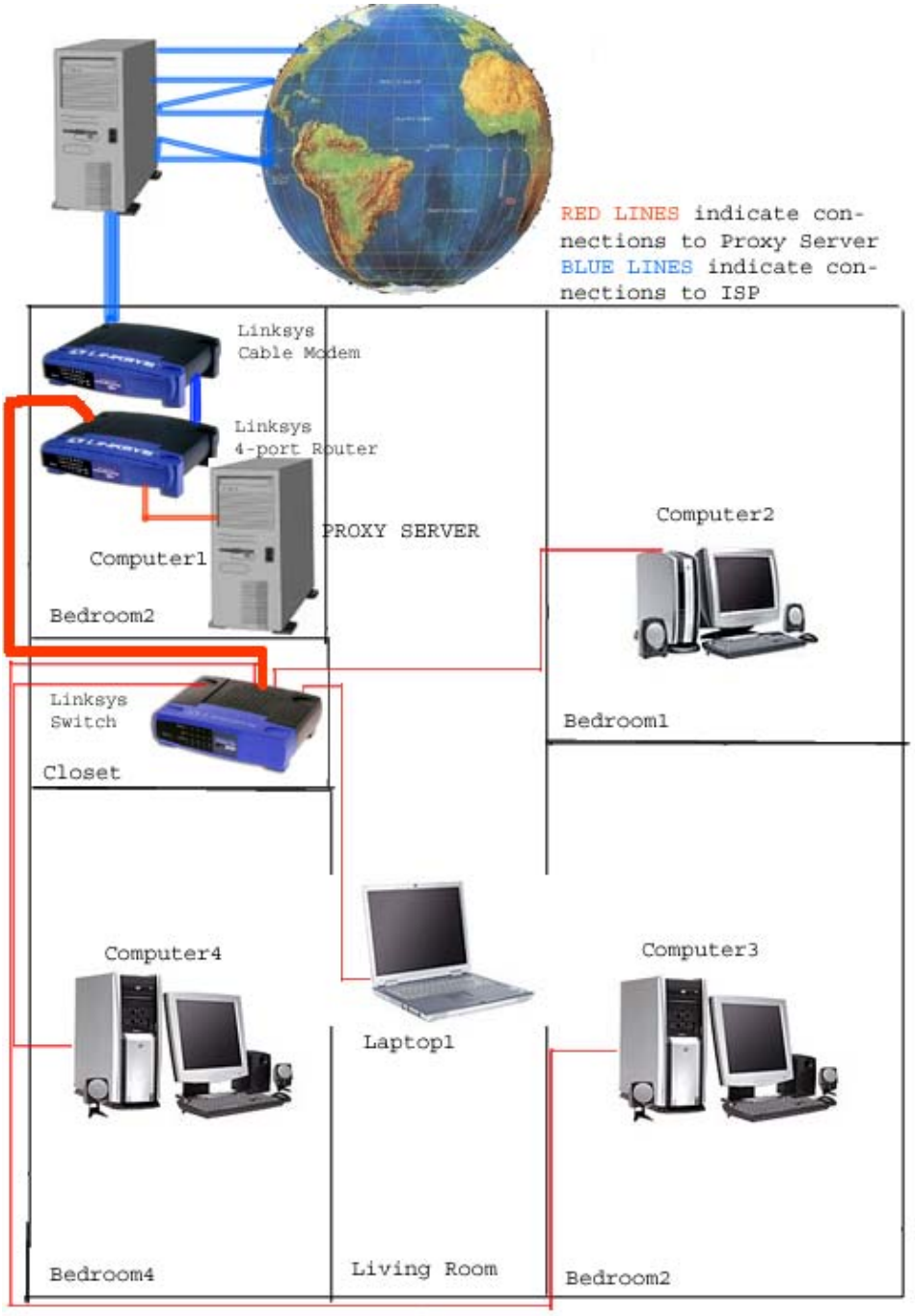
Proxy servers solve two main problems: security, and bandwidth. They enhance network security by filtering requests on the application level. They can be configured for authentication and breaking of any direct links with unwanted types of requests. By storing information in cached memory, proxy servers help conserve bandwidth and thus increase network speeds in the long run.

Some of the problems that use of proxy servers may cause are: availability of software, limited virus protection, abuse of anonymity, limited access to certain websites, ease of configurability, and compatibility.

Use of proxy servers can help businesses block access to unwanted websites. This can greatly conserve bandwidth and improve employee productivity. Hands-on

research results showed that use of proxy on a small network helped filter 95 % of unwanted content and accounted for higher download speeds in the long run.

Appendix 1


RED LINES indicate connections to Proxy Server
BLUE LINES indicate connections to ISP
Linksys Cable Modem
Linksys 4-port Router
PROXY SERVER
Computer1
Bedroom2
Computer2
Bedroom1
Linksys Switch
Closet
Computer4
Laptop1
Computer3
Bedroom4
Living Room
Bedroom2

Works Cited

[1] LITA Regional Institute. *Proxy Web Servers and Authentication.* February 22, 2001. November 19, 2002. < http://www.pandc.org/proxy>

[2] Journal Storage. *Remote* Authentication. September 14, 2001. November 17, 2002. <http://www.jstor.or/about/authentication.html>

[3] Watchguard Technologies. *Application Security Proxies.* November 18, 2002. < http://www.watchguard.com/products/proxy.asp>

[4] King, Nelson. *Proxy Server* Overview. May 30, 2002. November 16, 2002. <http://www.serverwatch.com/stypes/>

[5] Angel, Jonathan. *Proxy Servers*. April 1, 1999. November 15, 2002. <http://www.networkmagazine.com

[6] Public Proxy Servers. *Proxy Servers.* November 15, 2002. http://www.proxyservers.com

[7] Communications News. *Increase Web security and performance.* September 2002. Communications news, Vol. 39 Issue 9, page 44.

[8] Morgan, Lisa. *Filter it out*. April 17, 2000. InternetWeek, Issue 809, page 55.

[9] JANET-CERT. *Protecting Services*. November 15, 2002. <http://www.ja.net/CERT/JANET-CERT/prevention/services.html>

[10] Georgia Library Learning Online. *Guidelines for the use of proxy servers and filtering*. November 17, 2002. <http://www.usg.edu/galileo/download/Filter_and_Proxy_Guidelines.doc>

[11] Best Manufacturing Practices. *Firewalls and Proxy Servers*. April 29, 2002. November 14, 2002. <http://www.bmpcoe.org/sitehelp/firewalls.html>

[12] Purveyor Administrator's Guide. *Web Proxy Servers.* November 19, 2002. <http://vms.process.com>

[13] Media & Methods. *Internet Filtering*. March/April 2000. Media & Methods, Vol 36, Issue 4, Page 6.

[14] Reardon, Marguerite. *Caches keep content close at hand*. March 21, 1999. Data Communications. Vol. 28, Issue 4, Page 47.