# Information Security Management:

## Web Proxy Servers

**Billy Short**

**7/20/2016**

## TABLE OF CONTENTS

## Abstract

Information Technology management teams are constantly attempting to keep information safe and secure with various information security mechanisms. Most teams upgrade infrastructure by implementing new software and hardware devices, such as firewalls, demilitarized zone servers, or proxy servers to name a few. This writing will focus on defining what proxy servers are, what they are used for, why they are useful, advantages and disadvantages of implementing proxy servers, alternatives, and most importantly how they are used to enforce information security in order to keep data safe and secure. Throughout this document, I will include real world examples of how proxy servers are used, and explain some of the benefits of implementing one. By writing this document, I have learned quite a bit of information about proxy servers, and hope to help supply information to others who would like to learn more about this topic. We will focus on web proxy servers in particular throughout this writing.

## Introduction to proxy servers

What exactly is a proxy server? A proxy server can be generally defined as a computer acting as a gateway between a local area network and another larger network such as the internet ("Indiana University...). Basically, a proxy server acts as an intermediary device between a smaller network, such as a business network, to another network, which is typically the internet. Many times proxy servers are known as simply 'proxy', and this term will be applied throughout this writing. With a proxy, all data from one network is transferred through the proxy server and into the internet. This ensures that there are no direct connections from the inside of a network to the outside of the network, which limits access points in which hackers and attackers may exploit to gain access inside a local area network. This also helps keep internal IP addresses private, adding an extra layer of security to network infrastructure. Most proxy servers have similar functions, but typically are categorized as specific types, according to what their use is for in the network. For example, web proxies, or HTTP proxies route all client HTTP protocol traffic (access to web pages) to the web proxy. SMTP proxies rout all client SMTP protocol traffic (email) to the email proxy. There are many other types of proxies available for management use, but these tend to be the most commonly implemented, especially in an enterprise environment. For the duration of this report, we will focus on web proxies in particular.



## What do web proxies do?

Web proxies are very commonly implemented in all sorts of companies. Small, medium

and large organizations decide to implement proxy servers. What exactly do web proxies do? In this section we will address this question.

Information security management teams implement web proxies mainly due to security purposes. First, to better help readers understand the architecture of a web proxy in a simple network, please refer to **Figure 1.1**.

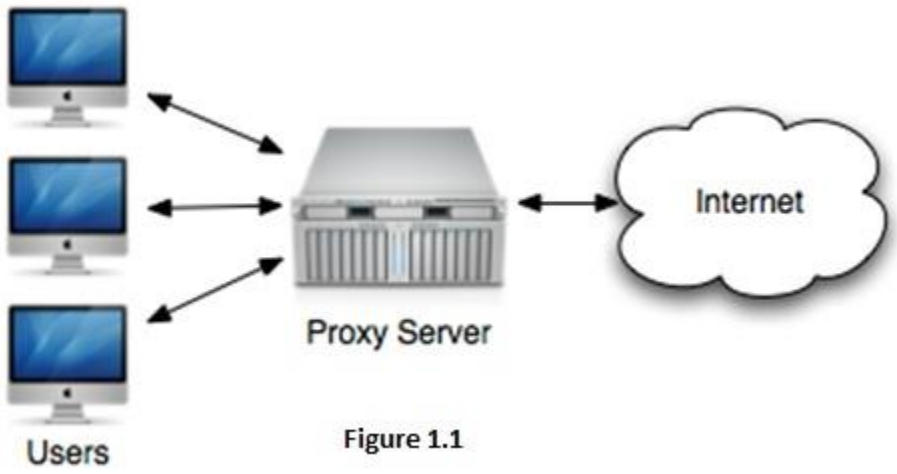


Figure 1.1

As mentioned in a previous section, a proxy server acts as an intermediary device, typically between a local area network (LAN) and a wide area network (WAN). In Figure 1.1, we see that the proxy server is in the middle of a simple small local area network of three users that are connecting to the internet. So what does a web proxy do while being an intermediary device between a LAN and WAN? Web proxies in particular handle network traffic, specifically HTTP protocol packets. Because a web proxy is in between a LAN and WAN (in this case), all network traffic from the three user clients will go pass through the proxy server and on to its destination. If a user is accessing the internet and they are retrieving a file, the requested files come from the internet and back into the proxy server, which then can be accessed by the user who requested the file. Web proxies are managed by an information security management team

which is typically a part of the organization that is implementing the proxy server. In stating this, web proxies are typically configured and managed locally by the organization, and not by internet service providers or other third party vendors. Because the web proxy is locally managed, companies are able to secure information and other user data much more effectively by limiting what and where users can access information from. This helps ensure that data stays safe and secure from potential attackers and other information breaches. Now that we have some information about how proxies fundamentally operate, we can then move along to how organizations typically use web proxies in an enterprise environment.

## Organizational uses

Regardless of size, many organizations implement some form of web proxy. Why do companies turn to web proxies to help secure information? That is just it, the main reason that companies implement web proxies is to help keep confidential data and information more secure. Many information technology management teams look at security as an onion. Nothing can be completely secure, but if you keep adding enough layers of security, it will help repel, slow down, prevent, or discourage potential attackers from trying to access secure data (Data Security Defense in Depth...). Web proxy implementation is just another layer of network security that is managed locally by the information security and technology management team. Although keeping secure data secure, there are other useful applications that organizations use web proxies for. Since all web traffic goes through a single web proxy server, network usage can be easily monitored by network administrators and other members of the IT team. This helps identify any sort of suspicious behavior that is occurring on the local network as well. Administrators may configure web proxies to only accept certain websites for the entire organization, can restrict

certain websites to specific users or groups, or can be used to block entire internet usage (***"RFC 5625 - DNS Proxy Implementation Guidelines***"). Many companies block ports that are known to be used for peer to peer (P2P) usage, such as BitTorrent (BitTorrent). P2P programs such as BitTorrent are used mainly for sharing files and folders very quickly to and from users around the world. Many times, these programs are used for sharing copyright protected information, such as music, movies, and software. By analyzing information gathered from a web proxy, administrators may be able to limit usage of these programs on a local area network. Some programs use specific ports for transmitting and receiving data, or are well known for using these specific ports. Administrators have the ability to configure the web proxy to block certain UDP or TCP port ranges so that users may not use P2P programs in an enterprise environment.

As mentioned above, web proxies are configured to transmit and receive all internet requests. Clients are configured to send and receive all packets directly to the proxy, which allows for effective and efficient monitoring of internet usage by the organization. Proxies are able to be applied to individual users, individual computers or workstations, or entire organizational units in Active Directory. Here is an example of how this could possibly work in an organization. Fred is a Network Administrator for a large manufacturing company. The plant manager - Thomas - is reviewing performance evaluations for other managers, and notices that one manager's - Ashley's - performance has steeply declined. All users sign a internet and computer usage form that states that all company issued computers must only be used for company/business usage only, as well as company resources such as internet and server access. While getting back to the issue at hand, Thomas is wondering what could be contributing to Ashley's steep decline in work performance. He reaches out to Fred and the IT management

team. Thomas wants daily reports of Ashley's internet usage to see if there is reasoning behind the sudden performance decrease. Fred pulls log files from the web proxy, as well as continue to monitor Ashley's internet usage for the next few weeks. After Fred gathers data, he passes it along to Thomas, and based on the data, it is apparent that Ashley is using her company issued computer for other personal uses, as well as accessing non-work related websites during working hours. Appropriate disciplinary actions could be determined and enforced based on policies set in place. Web proxies are not meant to get people in trouble at work, it is meant for businesses and organizations to have the means to ensure that company data and information is secure, and that company resources such as computers, laptops, and internet bandwidth are being used in compliance with company policies.

## Advantages and Disadvantages

Implementing web proxies have quite a few advantages for an organization. Some of these advantages are mentioned in the sections above. One of the biggest advantages that web proxies can offer to organizations is the central management and control in regards to network access. Administrators can restrict or grant access on an as-needed basis for users, computers, or groups of either.

Added security is also a major benefit to implementing a web proxy in between the local area network and a wide area network such as the internet. Because the proxy acts as an intermediary between the LAN and WAN, internal IP addresses are more secure. This is another layer of the security onion, as referenced earlier. Unless direct access is configured in the web proxy to allow a direct connection from the LAN to WAN, then potential attackers cannot get to

the internal network as easily in comparison to if the proxy was not implemented. If there was no proxy installed, which is still rather common, then Administrators would only rely on NAT (Network Address Translation), which transparently changes the origination address of traffic before passing it to the internet ("Indiana University....").

Although there are a lot of advantages for the IT management team in regards to network administration, web proxies also have disadvantages. Users can actually change internet settings if they are not locked into place. This could ultimately render the web proxy useless because the user is basically bypassing the proxy. These settings are can be accessed shown in **Figure 1.2.**

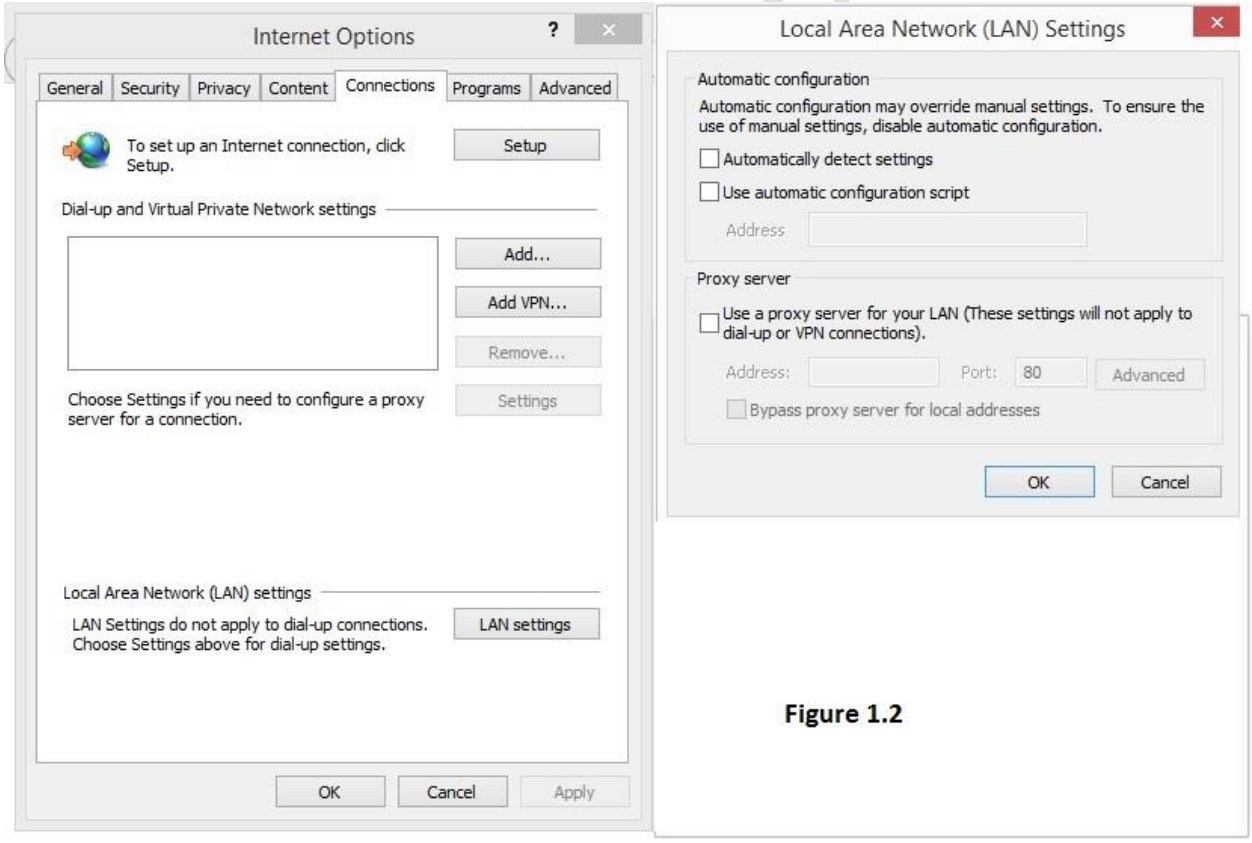


**Figure 1.2**

Without a group policy setting that blocks domain users from changing these LAN settings, users can just change these settings and bypass a configured web proxy (none of my boxes are checked because I am not currently using a proxy).

One major concern for web proxies is the fact that it many see it as a bottleneck in networks ("Eliminating the I/O Bottleneck from World Wide Web Proxies"). For example, a computer lab with fifteen students are accessing the same website at the same time for a research studies lab. The computers that the students are using are domain computers that have client settings that forward all network traffic to a configured web proxy. Because this is a domain, it is not only fifteen computers on the network, there are also hundreds of other domain computers and devices that are sending network traffic to the configured web proxy. With all of these packets being sent simultaneously through the web proxy to be filtered out, many see this as a bottleneck. A bottleneck in a network is defined as a condition where data flow is limited by computer or network resources ("Resolving Network Bottlenecks"). Most of the time, this is referring to network bandwidth. So how to most web proxies get around this bottleneck issue? Web proxies use advanced cache algorithms in order to create a cache on the proxy server. When users frequently access certain websites or web pages, the web proxy in essence takes note of this, and makes a cache of the location of this address. Instead of having compare what policies and restriction rules that are configured on the web proxy, the proxy automatically pushes the client to the local cache. This helps resolve issues with network bottlenecking at the web proxy server point (***"Proxy Cache Algorithms: Design, Implementation, and Performance"***). Although the proxy cache algorithm is meant to increase usability while keep information secure, some caches save passwords that are typed into accessed websites. This is essentially the same things as cookie files in an internet browser. There must be a

medium between security, speed and usability, and the local cache algorithms provided by the web proxy helps ensure just that.

Another disadvantage that information security management teams should ponder is the fact that managing various types of proxy servers is specialized training. This is why many companies bring in third party vendors to implement proxy servers. Specialized training to keep up with up to date information in regards to the selected implementation of the proxy server that a company chooses will need to be factored in. As more and more technology becomes available, administrators must stay current with security trends and other issues as it may affect the proxy server. More importantly, confidential data and information relies on well administrated infrastructure such as web proxies and firewalls.

## Alternatives

Although proxies are widely implemented in a variety of business types, some Information Security management teams may decide that a proxy server is not the right fit for their company. Many companies outsource most aspects of security and network management to third party vendors or offshore most hardware and software to datacenters. Since web proxies are locally managed, there would not be a need for a proxy server to be implemented by the IT team because everything would already be managed by the third party vendor, which would probably have some sort of web proxy in place and monitoring the company's infrastructure.

When used in conjunction with web proxies, firewalls can provide extremely secure networks to ensure confidential data stays secure. It helps provide information technology administrators with the resources to block any activity, grant access to certain websites, block

certain websites, and heavily monitor internet usage by connected clients (***Varanasi, Badhri, Remzi Arpaci Dusseau, and Paul Barford). The biggest difference between firewalls and proxy servers is that proxy servers more or less 'guide and control' traffic, mainly from clients to the proxy server, proxy server to internet, internet back to proxy server, and finally proxy server back to client. Firewalls tend to just restrict entire networks or complete access. Firewalls are more for defining what computers can access which networks, as with web proxies you can decide specifically what websites that computer or client can access. Firewalls are on a much larger scale than web proxies, but they both transmit and receive a lot of data. When working in tandem, information technology administrators can secure the network with a proxy server that controls traffic to computers, and the firewall maintain secure traffic to the network as a whole ("Difference Between Proxy Server & Firewall").

Regardless of whether a web proxy is implemented or not, a Virtual Private Network or VPN may be used. VPN's are configured to allow users to have a secure tunnel into a local area network from outside the network. For example, many companies have VPNs that their clients use in order to securely connect to the internal business network in order to access certain files they need, especially when they are not at the plant. This enables people to work from other locations, such as working at home, but still have the same access as if they were sitting at their desk inside the office. The reason VPN's are just an alternative to a proxy server is because they do not typically route through a proxy server, they are typically routed directly through configuration in the local area network firewall. Although clients are not forwarding all internet traffic through web proxies, clients may still be monitored via the firewall, and many times the VPN client itself has monitoring capabilities built in that an information security administrator may use to access and acquire more information about internet usage from clients.

## Open source proxy servers

Most enterprise web proxies are ongoing paid for service, or even outsourced to third party vendors. Aside from that, I was wanting to show a few examples of residential proxy servers that just about anybody can set up. Linux based proxy servers are abundant, but I wanted to focus on two in particular. Squid is a widely used proxy server that people can build and use with their home network. Squid is a cache web proxy, which as mentioned above means that it learns websites that users frequently use in order to help alleviate any bottlenecking issues in the network ("Squid-cache.org").

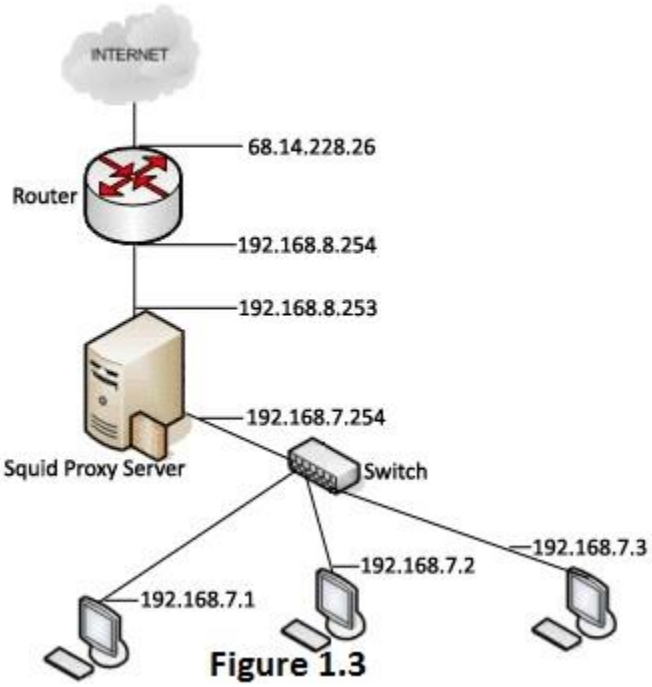

Figure 1.3

In **Figure 1.3**, you can see that Squid is installed in this network. The proxy server is installed directly between the switch that connects all the users together. The users are in the 192.168.7.0

network, but those IP addresses cannot be seen very easily from the outside network due to all traffic from the proxy server being on 192.168.8.0 network. This helps keep the 192.168.7.0 network more secure because those IP's are being translated twice, once from the LAN to the proxy server, and then from the proxy server to router transferred to the WAN (internet). Linux provides mostly free open source software that can be locally installed just about anywhere. There are many alternatives to Squid, such as Polipo, Varnish, Privoxy, Apache Traffic Server, and so on.

## Conclusion

While writing this report, I learned quite a bit of information that I did not know of before about proxy servers. Web proxies are abundantly used in many different types of businesses, ranging from small to large. There are many benefits to implementing a web proxy in an enterprise environment, including keeping data safe and secure, increasing layers of security, monitoring network bandwidth usage, spotting possible network issues early, and ensuring that employees use company assets for business purposes during working hours. We also discussed how web proxies work, where they are typically located in a network, why they are implemented by businesses, and advantages and disadvantages. I believe we will continue to see proxy servers increase more and more as we go into the future, especially since more and more devices are connecting to the internet. More devices directly relates to internet bandwidth. Web proxies help ensure that bandwidth is being used as it should, and most importantly helps keep confidential data and information safe and secure.

## Bibliography

"Indiana University Indiana University Indiana University." *What Is a Proxy Server?* N.p., n.d. Web. 8 July 2016.

***"RFC 5625 - DNS Proxy Implementation Guidelines." *RFC 5625 - DNS Proxy Implementation Guidelines*. N.p., n.d. Web. 8 July 2016.

***"Proxy Cache Algorithms: Design, Implementation, and Performance." *Proxy Cache Algorithms*. N.p., n.d. Web. 9 July 2016.

"Data Security Defense in Depth: The Onion Approach to IT Security." *Security Intelligence*. N.p., 15 Jan. 2015. Web. 9 July 2016.

"BitTorrent." *BitTorrent*. N.p., n.d. Web. 10 July 2016.

"Eliminating the I/O Bottleneck from World Wide Web Proxies." *Eliminating the I/O Bottleneck from World Wide Web Proxies*. N.p., n.d. Web. 10 July 2016.

***Varanasi, Badhri, Remzi Arpaci Dusseau, and Paul Barford. *NFS Proxies: Design, Implementation and Applications*. Thesis. University of Wisconsin, n.d. N.p.: n.p., n.d. Print.

"Resolving Network Bottlenecks." *Resolving Network Bottlenecks*. N.p., n.d. Web. 10 July 2016.

"Proxy Server - It's Advantages & Disadvantages." *RS Web Solutions*. N.p., 06 Feb. 2016. Web. 1 July 2016.

"What Are the Benefits of Using a Proxy?" *HowTo Geek RSS*. N.p., n.d. Web. 10 July 2016.

"Differences Between 3 Types Of Proxy Servers: Normal, Transparent And Reverse Proxy." *Web Upd8 Ubuntu Linux Blog Summaryonly*. N.p., n.d. Web. 1 July 2016.

"Implementing Proxy Server." *Implementing Proxy Server*. N.p., n.d. Web. 1 July 2016.

"Design of an HTTP Proxy Server." *Academia.edu*. N.p., n.d. Web. 1 July 2016.

"Simple Questions: What Is a Proxy Server & Why Would You Use One?" *Digital Citizen*. N.p., n.d. Web. 8 July 2016.

"Difference Between Proxy Server & Firewall." *Tech in*. N.p., n.d. Web. 8 July 2016.

"Squid-cache.org." *Squid : Optimising Web Delivery*. N.p., n.d. Web. 12 July 2016.