A STUDY OF RECENT RESEARCH TRENDS OF PROXY SERVER

Yogita Chhabra

Assistant Professor, Department of Information Technology, Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh Technical University, Lucknow (India)

ABSTRACT

A proxy server is a kind of buffer between your computer and the Internet resources we are accessing (Web sites, FTP archives etc.). The data we request come to the proxy first, and only then it transmits the data to us. Any web site in the world can track your movements through its pages and monitor your reading interests using our IP address, a unique ID assigned to each computer on the Internet. Depending on the policies of the Internet resource, we might not be able to get access to the information we need. Using only our IP address and the information about our operating system, a Web site can automatically exploit security holes in our system using some not-very-complex, ready-made, free hacking programs. A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client's request or the server's response for various purposes. In this paper discuss a proxy server, need to use a proxy server, purpose, different types of proxies server, advantages, purpose of proxy server, performance etc..

Keywords: Gateway, HTTP Authentication, Network Security, Protocol, Web Server

I. INTRODUCTION

A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server. Some home networks, corporate intranets, and Internet Service Providers (ISPs) use **proxy servers** (also known as **proxies**). Proxy servers act as a "middleman" or broker between the two ends of a client/server network connection by intercepting all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server. Proxy servers work well between Web browsers and servers, or other applications, by supporting underlying network protocols like HTTP.

A proxy server is computer that makes request for a client. Proxy servers are used to get past filters. Filters usually don't recognize proxy servers and the sites they visit are usually allowed. So if we are ever behind a filter try to use a proxy server to go to the websites that we want to visit.

In computer networks, a proxy server is a server (a computer system or an application program) that services the requests of its clients by forwarding requests to other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server provides the resource by connecting to the specified server and requesting the service on behalf of the client [1]. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server. In this case, it would 'cache' the first request to the remote server, so it could save the information for later, and make everything as fast as possible. A proxy server that passes all requests and replies unmodified is usually called a gateway or sometimes tunnelling proxy.

A proxy server can be placed in the user's local computer or at various points between the user and the destination servers or the Internet. With the fast development of network, the network issues such as viruses, attacks, hacks are increasing day by day. So network monitor and analysis is becoming more and more necessary now a days.

II. USES

A proxy server has a large variety of potential purposes, including:

1. To keep machines behind it anonymous, mainly for security [3].
2. To speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server [4].
3. To apply access policy to network services or content, e.g. to block undesired sites.
4. To log/audit usage, i.e. to provide company employee Internet usage reporting.
5. To bypass security / parental controls.
6. To circumvent Internet filtering to access content otherwise blocked by governments [6].
7. To scan transmitted content for malware before delivery.
8. To scan outbound content, e.g., for data leak protection.
9. To allow a web site to make web requests to externally hosted resources (e.g. images, music files, etc.) when cross-domain restrictions prohibit the web site from linking directly to the outside domains.

A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes tunnelling proxy. A proxy server can be placed in the user's local computer or at various points between the user and the destination servers on the Internet.

A reverse proxy is (usually) an Internet-facing proxy used as a front-end to control and protect access to a server on a private network, commonly also performing tasks such as load-balancing, authentication, decryption or caching.

III. PURPOSE

Proxy servers have two main purposes

3.1 Improve Performance

Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. Consider the case where both user X and user Y access the World Wide Web through a proxy server. First user X requests a certain Web page, which we'll call Page 1. Sometime later, user Y requests the same page. Instead of forwarding the request to the Web server where Page 1 resides, which can be a time-consuming operation, the proxy server simply returns the Page 1 that it already fetched for user X. Since the proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers support hundreds or thousands of users. The major online services such as America Online, MSN and Yahoo, for example, employ an array of proxy servers.

3.2 Filter Requests

Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites.

IV. WHY WE NEED TO USE PROXY SERVERS?

4.1 Transfer Speed Improvement

If the file we requested was received before to our proxy server, then proxy server will interrupt this file request and we will receive the file directly from proxy. However need to know, we can got the "speed down" effect. This effect appears when our proxy has long answer time because there is slow connection between us and our proxy server.

4.2 Security and Privacy

An anonymous proxy destroys information about our computer in the requests header. So we can safely surf the net and our information will never be used by hackers and spammers.

Sometimes we encounter some problems while accessing to web server (for example, web-chat). We have mistaken while working with some data and/or the server administrator restricted access from our IP. So we can use the anonymous proxy and try to access again.

V. ADVANTAGES

1. For security reasons it will keep the machine anonymous most of the time
2. It will enhance the speed to access the concerned resources. As far as web proxies are concerned it can be used to cache the web pages directly from a web server.
3. It will apply the access policy for the networks services as well as content. It can block the unwanted sites.
4. It can bring you log or audit related usages.
5. It can offer you top security and parental controls.
6. It can scan the outbound content effectively and can protect your data.
7. Proxy servers can be used for circumventing regional restrictions.

Proxy server works like a firewall because we are not connected directly to the internet, if we connect to that particular website through proxy server; this anonymous proxy server will isolate us from the site but still give we internet access. We can surf securely

VI. CATEGORIES

There are many different types of proxy servers out there, but following are some commonly known proxies.

6.1 Anonymous Proxy

An anonymous proxy server also known as web proxy generally attempts to anonymize web surfing by hiding the original IP address of the end user. This type of proxy server are typically difficult to track, and provides reasonable anonymity for most users.

6.2 Distorting Proxy

This type of proxy server identifies itself as a proxy server, but make an incorrect original IP address available through the http headers.

6.3 High Anonymity Proxy

This type of proxy server does not identify itself as a proxy server and does not make available the original IP address. High anonymity proxies, only include the REMOTE_ADDR header with the IP address of the proxy server, making it appear that the proxy server is the client.

6.4 Intercepting Proxy

An intercepting proxy, also known as a transparent proxy, combines a proxy server with a gateway. Connections made by client browsers through the gateway are redirected through the proxy without client-side configuration. These types of proxies are commonly detectable by examining the HTTP headers on the server side.

6.5 Reverse Proxy

A reverse proxy is another common form of a proxy server and is generally used to pass requests from the Internet, through a firewall to isolated, private networks. It is used to prevent Internet clients from having direct, unmonitored access to sensitive data residing on content servers on an isolated network, or intranet. If caching is enabled, a reverse proxy can also lessen network traffic by serving cached information rather than passing all requests to actual content servers.

6.6 Transparent Proxy

A transparent proxy is a server that satisfies the definition of a proxy, but does not enforce any local policies. It means that it does not add, delete or modify attributes or modify information within messages it forwards. These are generally used for their ability to cache websites and do not effectively provide any anonymity to those who use them. However, the use of a transparent proxy will get you around simple IP bans. Further, your web browser does not require special configuration and the cache is transparent to the end-user. This is also known as transparent forward proxy.

VII. ISSUES

The diversion / interception of a TCP connection create several issues. Firstly the original destination IP and port must somehow be communicated to the proxy. This is not always possible (e.g. where the gateway and proxy reside on different hosts). There is a class of cross site attacks which depend on certain behaviour of intercepting proxies that do not check or have access to information about the original (intercepted) destination. This problem can be resolved by using an integrated packet-level and application level appliance or software which is then able to communicate this information between the packet handler and the proxy.

Intercepting also creates problems for HTTP authentication, especially connection-oriented authentication, such as NTLM (NT LAN Manager), since the client browser believes it is talking to a server rather than a proxy. This can cause problems where an intercepting proxy requires authentication, then the user connects to a site which also requires authentication.

Finally intercepting connections can cause problems for HTTP caches, since some requests and responses become uncacheble by a shared cache. Therefore intercepting connections is generally discouraged. However due to the simplicity of deploying such systems, they are in widespread use.

VIII. DETECTION

There are several methods that can often be used to detect the presence of an intercepting proxy server:

1. By comparing the client's external IP address to the address seen by an external web server, or sometimes by examining the HTTP headers received by a server. A number of sites have been created to address this issue, by reporting the user's IP address as seen by the site back to the user in a web page [2].
2. By comparing the sequence of network hops reported by a tool such as trace route for a proxied protocol such as http (port 80) with that for a non proxied protocol such as SMTP (port 25) [3][4].
3. By attempting to make a connection to an IP address at which there is known to be no server. The proxy will accept the connection and then attempt to proxy it on. When the proxy finds no server to accept the connection it may return an error message or simply close the connection to the client. This difference in behaviour is simple to detect. For example most web browsers will generate a browser created error page in the case where they cannot connect to an HTTP server but will return a different error in the case where the connection is accepted and then closed [5].

IX. CONCLUSIONS

A proxy server is a machine that accepts incoming web requests and then forwards them on to the destination. They are an intermediary of the internet and keep your computer and destination web server separate. The proxy concept was invented in the early days of distributed systems as a way to simplify and control their complexity. Today, most proxies are a web proxy, allowing access to content on the World Wide Web. A proxy server can be placed in the user's local computer or at various points between the user and the destination servers on the Internet. A proxy server is a benefit for administration, because the network administrator can filter and a manage Internet usage from one machine. All users access the Internet from the proxy server, so network administrators can block certain pages and limit the amount of accessible websites. This type of filtering is usually done by large businesses that need to limit websites either individually or through categories. A proxy server protects the network from malware, which is installed on users' computers when they access an infected website. When the malware is installed on the user's machine, it can spread to other machines on the network.

REFERENCES

[1] Mitchell, Bradley. "Proxy Servers Tutorial - About Proxy Servers." About.com: Wireless/Networking. 2007.

[2] Shapiro, Marc (May 1986). "Structure and encapsulation in distributed systems: the Proxy Principle". Int. Conf. on Distributed Computer Sys.: 198-204. Retrieved 4 September 2011.

[3] "Firewall and Proxy Server HOWTO" tldp.org. http://tldp.org/HOWTO/Firewall-HOWTO-11.html. Retrieved 4 September 2011. "The proxy server is, above all, a security device."

[4] Thomas, Keir (2006). Beginning Ubuntu Linux: From Novice to Professional. Apress. ISBN 9781590596272. "A proxy server helps speed up Internet access by storing frequently accessed pages".

[5] Wessels, Duane (2004). Squid The Definitive Guide. O'Reilly. pp. 130. ISBN 9780596001629.

[6] "2010 Circumvention Tool Usage Report". The Berkman Center for Internet & Society at Harvard University.

October2010. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

[7] “The Advantages of a Proxy Server”, eHow.com http://www.ehow.com/list_5907691_advantages-proxy-server.html#ixzz1ZF0XCl47