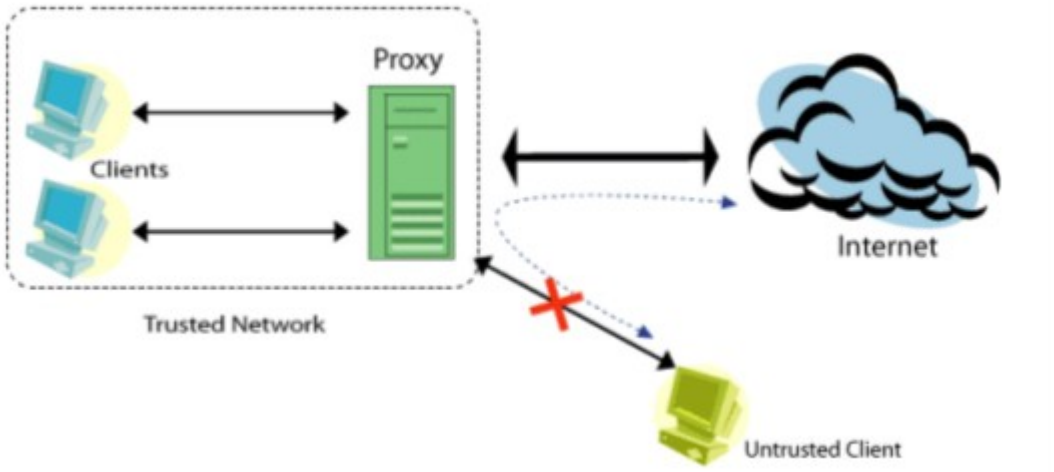
Open Proxy Servers

Index

What is a Proxy Server?

A proxy server acts as an intermediary between a client computer and the Internet serving as a buffer between the client computer and the Internet resources one is accessing.



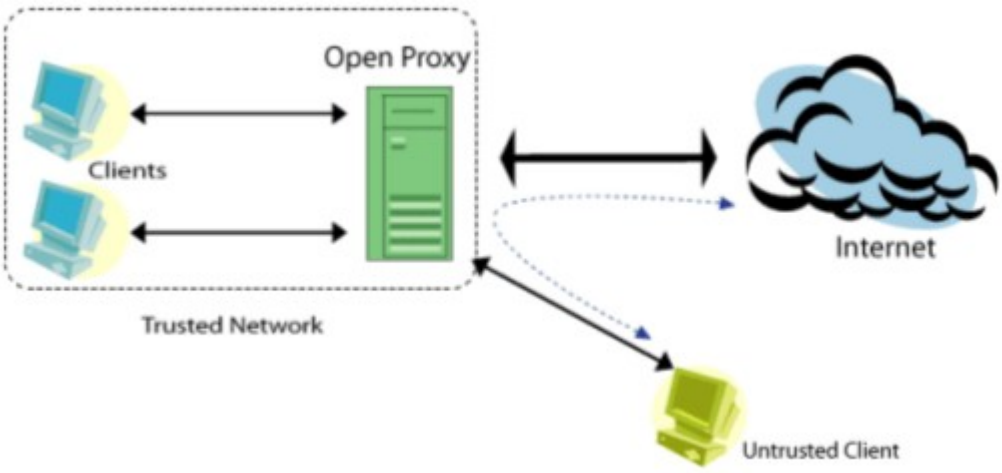
When a client makes a request for an Internet resource through a proxy server, the proxy makes a connection to the requested resource on the client's behalf to get the resource and delivers it down to the client. By this process, it is able to hide the internal address of the client to the Internet and the IP address of the proxy only becomes visible on the Internet.

A Proxy Server can be used to enforce security, administrative control, and caching. A normal Web browser must be configured to use the proxy either manually or with a configuration script. A transparent proxy combines a proxy server with NAT so that connections are routed into the proxy without client-side configuration.

Proxies usually operate on the following ports ranges : 80, 81, 8000, 8080 (HTTP CONNECT), 1080 (SOCKS), 3128 (Wingate/Squid), 6588 (AnalogX).However, other ports can be used for the same purposes but are less common.

What is an Open Proxy Server?

A Proxy Server should accept requests from only its own clients by either forcing a client to connect from a range of IP addresses, or by using authentication. Any proxy server that doesn't restrict its client base to its own set of clients and allows any other client to connect to it, is known as an open proxy. An open proxy will accept client connections from any IP address and make connections to any Internet resource. Open Proxy Servers act as blind intermediary to any other network addresses without any authentication.



An Open Proxy Server commonly allows HTTP access but it can also be used for ftp, Usenet, email (including spam), IRC/instant messaging or even launch a DoS attack.

Exploitation of Open Proxy Servers

A malicious user can effectively hide his own IP address by using an Open Proxy Server for illegal activities like hacking. In such scenario instead of the IP address of the attacker appearing in the log files of the attacked system, the IP address of the Open Proxy Server shall appear. Malicious users routinely chain through several such Open Proxy Servers making it difficult to trace back to the origin of the user.

Though, Open Proxy Servers are not the same as open SMTP relays, they are infact a far more serious problem, since they allow traffic for virtually any network service to be bounced/ tunneled through the host.

An Open Proxy Server can be used by a spammer as a spam conduit to anonymously send out spam, using the resources of the owner of the proxy. The use of Open Proxy Server complicates the tasks of both filtering Spam and tracking spammers.

Consequences of Open Proxy Servers

An Open Proxy Server in an organization can lead to-

- The IP of the organization being blacklisted by various bodies
- The loss of image of the organization, if misused for illegal activities
- Legal ramifications, if misused for illegal activities
- Loss of bandwidth
- It may also serve as a conduit for inbound attacks, completely bypassing a site's firewall architecture.
- It may also result in an increased risk of that host (and its network) getting scanned for other vulnerabilities

Legal Impact of maintaining proxy Servers knowingly /unknowingly

Connections made via an Open Proxy Server are often non-accountable, since the proxy may be doing no logging, or if logging is being done, logs may be unavailable to those investigating network incidents. Malicious users further cover their tracks by chaining through multiple proxies either manually or using products such as ProxyChains

Security Risks of using Open Proxy Servers

When a client system is using an Open Proxy Server to access the Internet, all the traffic flowing through the Open Proxy Server could be intercepted and possibly misused. These could include email messages, passwords or other sensitive information passing through the Open Proxy Server.

Common mistakes making a proxy open

Often, a proxy server is 'open' because it has not been configured correctly. The administrator who configured the server was probably not aware of the potential problems and security risks. It is very common for a novice administrator to set up a proxy with access rights that allows anyone to connect.

A proxy server may be ‘Open' due to the following:

- Improperly configured proxy server.
- Proxy administrator unaware of the dangers of leaving the proxy server ‘Open' .
- Inherent application deficiency.
- A conscious decision on the part of the party installing the proxy to run it open(compromised systems, political motivations, etc.)
- Administrator is unaware that a proxy server has been installed on his server by default while installing some other software or application.

Testing for an Open Proxy Server

The test to determine whether a proxy server is an Open Proxy Server has to be performed from outside the allowed client base. Therefore the test usually has to be carried out from outside the organizationalnetwork, to determine whether it is really 'open'. The easiest way to check an Open Web Proxy is to use the proxy settings in the client browser and try to connect to an Internet resource from outside the organizational network, using these settings. A successful connection would indicate that the proxy server is an Open Proxy Server.

There are also several sites where a proxy server could be tested on whether it is a Open Proxy Server. Some of the sites where they can be tested are:

Web-based Proxy Checkers

- http://defcon.one.pl/checker
- http://www.richard.zonnet.nl/cgi-bin/nph-proxycheck
- http://www.checker.freeproxy.ru/checker/
- http://www.dailyproxy.com/proxy_check.php
- http://spamlinks.openrbl.org/tools-proxy.htm#web

There are also several tools and scripts available to help test open proxy servers. A small listing is available in the following pages.

Proxy Checker Script/Tools

- **http://spamlinks.openrbl.org/tools-proxy.htm#scripts**
- **http://spamlinks.openrbl.org/tools-proxy.htm**
- **http://www.stayinvisible.com/index.pl/testing_software**

Open Proxy Server lists

Lists of Open Proxy Servers can be found easily with a simple web search. These lists are frequently updated, and some even include bandwidth statistics about each server. This list is continuously checked and kept updated, making the Open Proxy Servers easily accessible to malicious users.

Remedy for an Open Proxy Server

If a system is found to be running an open proxy, it needs to be removed immediately. The Proxy should be configured so that the clients allowed to connect through it are restricted only to IP addresses of its own trusted set of clients. Authentication should also be used to avoid misuse of the Proxy.

The details of fixing an Open Proxy Server vary based on the proxy software that is being used. The appropriate configuration guides and the vendors may be consulted to fix the open proxy. The following website lists details of fixing some common Proxy servers.

Fixing Open Proxies
http://spamlinks.openrbl.org/proxy-fix.htm

References

1. Abuse-Proxy (http://www.cyberabuse.org)

2. ProxyChains (http://proxychains.sourceforge.net/)

3. The Dangers Of Open Proxy Servers (http://theproxyconnection.com/openproxy.html)

4. Open Proxy Servers (http://www.postcastserver.com/help/Open_Proxy_Servers.aspx)

5. Exposing the Underground: Adventures of an Open Proxy Server (http://www.lurhq.com/proxies.html)

6. Open Proxy Servers: A Growing Source of Spam (http://cc.uoregon.edu/cnews/fall2002/openproxy.html)