FORWARD proxy

Forward proxy sits between internet and client

Most discussion of web proxies refers to the type of proxy known as a "forward proxy."

The proxy event, in this case, is that the "forward proxy" retrieves data from another web site on behalf of the original requestee.

For an example, I will list 3 computers connected to the internet.

* X = your computer, or "client" computer on the internet
* Y = the proxy web site, proxy.example.org
* Z = the web site you want to visit, [www.example.net](http://www.example.net)

Normally, one would connect directly from X --> Z.

However, in some scenarios, it is better for Y --> Z on behalf of X, which chains as follows:

X --> Y --> Z.

Reasons why X would want to use a forward proxy server:

Here is a (very) partial list of uses of a forward proxy server:

1) X is unable to access Z directly because

a) Someone with administrative authority over X's internet connection has decided to block all access to site Z.

Examples:

* The Storm Worm virus is spreading by tricking people into visiting familypostcards2008.com, so the system administrator has blocked access to the site to prevent users from inadvertently infecting themselves.
* Employees at a large company have been wasting too much time on facebook.com, so management wants access blocked during business hours.
* A local elementary school disallows internet access to the playboy.com website.
* A government is unable to control the publishing of news, so it controls access to news instead, by blocking sites such as wikipedia.org. See [TOR](https://www.onion-router.net/) or [FreeNet](https://freenetproject.org/).

b) The administrator of Z has blocked X.

Examples:

* The administrator of Z has noticed hacking attempts coming from X, so the administrator has decided to block X's IP address (and/or netrange).
* Z is a forum website. X is spamming the forum. Z blocks X.

Advantage  
- protect the clients identity

- bypass browsing restrictions

- block access to certain content

REVERSE proxy

Reverse proxy sits between internet and web servers

For this example, I will list three computers connected to the internet.

* X = your computer, or "client" computer on the internet
* Y = the reverse proxy web site, proxy.example.com
* Z = the web site you want to visit, [www.example.net](http://www.example.net)

Normally, one would connect directly from X --> Z.

However, in some scenarios, it is better for the administrator of Z to restrict or disallow direct access and force visitors to go through Y first. So, as before, we have data being retrieved by Y --> Z on behalf of X, which chains as follows: X --> Y --> Z.

What is different this time compared to a "forward proxy," is that this time the user X does not know he is accessing Z, because the user X only sees he is communicating with Y. The server Z is invisible to clients and only the reverse proxy Y is visible externally. A reverse proxy requires no (proxy) configuration on the client side.

The client X thinks he is only communicating with Y (X --> Y), but the reality is that Y forwarding all communication (X --> Y --> Z again).

Reasons why Z would want to set up a reverse proxy server:

1) Z wants to force all traffic to its web site to pass through Y first.

a) Z has a large web site that millions of people want to see, but a single web server cannot handle all the traffic. So Z sets up many servers and puts a reverse proxy on the internet that will send users to the server closest to them when they try to visit Z. This is part of how the Content Distribution Network (CDN) concept works.

Examples:

* [Apple Trailers](https://www.apple.com/trailers/) uses [Akamai](https://www.akamai.com/)
* Jquery.com hosts its JavaScript files using [CloudFront CDN](https://aws.amazon.com/s3/) ([sample](https://static.jquery.com/files/rocker/scripts/custom.js)).etc.

2) The administrator of Z is worried about retaliation for content hosted on the server and does not want to expose the main server directly to the public.

a) Owners of Spam brands such as "Canadian Pharmacy" appear to have thousands of servers, while in reality having most websites hosted on far fewer servers. Additionally, abuse complaints about the spam will only shut down the public servers, not the main server.

In the above scenarios, Z has the ability to choose Y.

Advantage  
- protects web server (harder to get targeted by DDOS attack)

- load balancer

- caching (static content)

- handle SSL encryption