Computer Networks

Proxy Server

What is it?

* Stands in between the client & the server.
* The client communicates with the proxy and the proxy communicates with the server.
* The client cannot inject the website server directly.
* When devices on the outside have to communicate with inside, they use proxy server.
* " " inside have to communicate with outside, they use reverse proxy server.
* Proxy server can also add functionality and security. Keep logs of all the network activities / traffic.

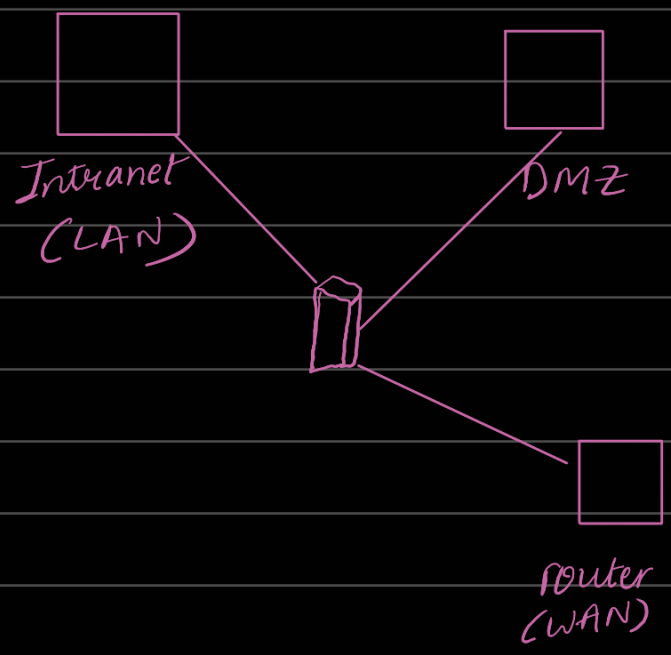
* Proxy Server makes it easier to monitor.
* Very easily turn on logging.
* Proxy server gives the illusion of inside communicating with the outside directly.
* Proxy servers are used to increase performance.
* We also can teach non-technical people to use proxy servers. The ability by which managers can block certain sites by themselves.
* Control the foubidden Websites in an organization.

ACLs are complicated, we block based on the datagream. Some sites can add/change IP addresses. We block all IP addresses using proxy servers.

* Proxy servers gives us more control on the internet.
We can better monitor using proxy servers.
* DMZ work in conjunction of proxy and reverse proxy.
* Reverse proxy are servers on the inside which want to communicate with outside devices.
* We can do these for E-Mail servers, FTP protocol.

What is a DMZ?

It is an area which is not on the same network.
Demilitarized zone allows an organization to access any untrusted networks such as the internet while ensuring its private network or LAN are protected.



* Devices on the outside get the illusion of communicating with the inside and get the functionality they need.
* Even desktop devices can't communicate with the outside.
* Monitor everything.

Created DMZ for extra layer of security.
DMZ is just another Local Area Network. It's a buffer between inside and the outside.

Benefits of using DMZ:-
Enable Access Control

Prevent Network reconnaissance

Blocking Internet Protocol Spoofing
Any attempt of attack will trigger alarms. By the time the attackers get to the second firewall, it will completely shut down the part where it connects to lets say an email server and not the whole Local Area Network. (Intrusion prevention system). Selectively shut down parts of the network.

* Read about the Conficker Virus