

Computer Networks – Fall 2020
Momina Atif Dar P180030

Report on Proxy, VPN and Containers

Proxy (application-level gateway):

Proxy server is used in homes as well as organizations and works on Transport Layer. It acts as a shield and protects the identity of user. If a user is using proxy and they request a webpage, the webpage is not directly delivered to user but it is sent to proxy server first, the proxy server may encrypt the data and send it to user. Proxy Server protects one's identity by changing the location and IP address of user. This way no malicious website or adversary can know the actual location and IP of user. Proxy Server can change user's IP address as well. Some pros of using IP address are to monitor the internet usage by employees or children, if people in authority want they can either block sites or allow sites but monitor the time spent on such sites. Even if user wants to protect their identity or keep their browsing history private they may use proxy as well. Proxy server caches data so the retrieval of webpages take less time than usual. Using proxy, users can also access websites or resources that are restricted in their country/region. For example some years ago when YouTube was banned in Pakistan, people started using proxy to access YouTube.

Where there are pros, there are cons as well. Some free proxy servers are questionable as they may not be using encryption technique or some may be fraud. Encryption is essential to protect user's personal data such as credit card numbers or passwords. No encryption would mean user's data is in plain text. Another con is logging. Some proxy servers log so they can sell data.

There are two types of proxy servers; forward proxy and reverse proxy. Forward proxy ensures no website communicates directly with user while Reverse proxy ensures no user communicates directly with web servers.

VPN (Virtual Private Network):

VPN kind of works the same as Proxy. It hides the IP of user. But proxy acts as a gateway whereas VPN creates a secure tunnel for users by replacing your ISP routing. It works on Operating System level which means that it redirects traffic coming from websites as well as applications. It also encrypts all of your data. When user wishes to connect to an open WIFI it's better to use VPN so somebody else can not look into or steal their data. VPN, unlike proxy, doesn't log so no more threat of user's personal data being sold. It also protect users from ISP tracking, government surveillance and hackers. But still there are some VPN service providers which do log.

Containers:

Containers in docker provide a light weight isolated environment to softwares so they can run fast. No matter on what OS the software runs, user doesn't have to install full-fledged OS just for the software, instead it installs an image of the needed OS. Multiple containers of same or different OS's can run at a time on host machine. The main advantage of containers is portability, user can easily port container from one system to another.

Containers are better than VMs because they are light weight and use way lesser resources than VMs, a server can host way more containers than VMs, containers start up easily while VM take time to boot up its OS's.

Another main advantage of containers is that they can be useful in splitting up the project in modules, for example, one container for database and another one for apache server. Inter-container communication can be established easily as well with the help of some commands.

It's important to pull images from trusted and authentic sources and verify it by SHA-256 code.

In containers, user can apply read-only environment which will nullify attacks that rely on uploading backdoors is in containers and this in turn ensures security.
