SSH Port forwarding (Port Forwarding/Tunneling)

- **port forwarding(redirection)** or **port mapping** is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.
- For example, if you are using a Linux/Unix system as a firewall you can redirect connections to port **1234** to an internal address such as **192.168.1.10:22** to provide an ssh tunnel from the outside world to an internal machine.
- In the following examples, you will get a shell prompt once the forwarding is complete. Keep this shell open to use the port forward and exit it whenever you want to stop the port forward.
  1. This command will forward port 8000 on your local machine to port 80 on www.kernel.org:

     ```
     ssh -L 8000:www.kernel.org:80user@localhost
     ```

     Replace user with the username on your local machine.
  2. This command will forward port 8000 on a remote machine to port 80 of www.kernel.org:

     ```
     ssh -L 8000:www.kernel.org:80user@REMOTE_MACHINE
     ```

     Here, replace REMOTE_MACHINE with the hostname or IP address of the remote machine and user with the username you have SSH access to.

Types of Port Forwarding

There are three varieties of port forwarding:

1. Local Port Forwarding

Users can securely pass data and information from a client application operating on the same computer as a Secure Shell (SSH) client thanks to local port forwarding, enabling connections from their local machines to other servers.

Any application operating from this server-side can access services on the SSH client-side because this protocol conducts all its activities at the SSH level. This port forwarding technique serves the same purpose as tunneling methods and protocols. This can get around firewalls that restrict access to specific websites.

2. Remote Port Forwarding / Reverse port Forwarding

Any user on the distant server can connect to a TCP port using this port forwarding. The most frequent users of remote port forwarding are remote workers connecting from their homes to a secure server and establishing external access to an internal web server.

- Reverse port forwarding is one of the most powerful features of SSH. This is most useful in situations where you have a machine which isn't publicly accessible from the Internet, but you want others to be able to access a service on this machine.
- In this case, if you have SSH access to a remote machine which is publicly accessible on the Internet, you can set up a reverse port forward on that remote machine to the local machine which is running the service.

```
ssh -R 8000:localhost:80 user@REMOTE_MACHINE
```

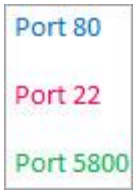
- This command will forward port `8000` on the remote machine to port `80` on the local machine. Don't forget to replace `REMOTE_MACHINE` with the hostname of the IP address of the remote machine.
- Using this method, if you browse to `http://localhost:8000` on the remote machine, you will connect to a web server running on port `80` of the local machine.

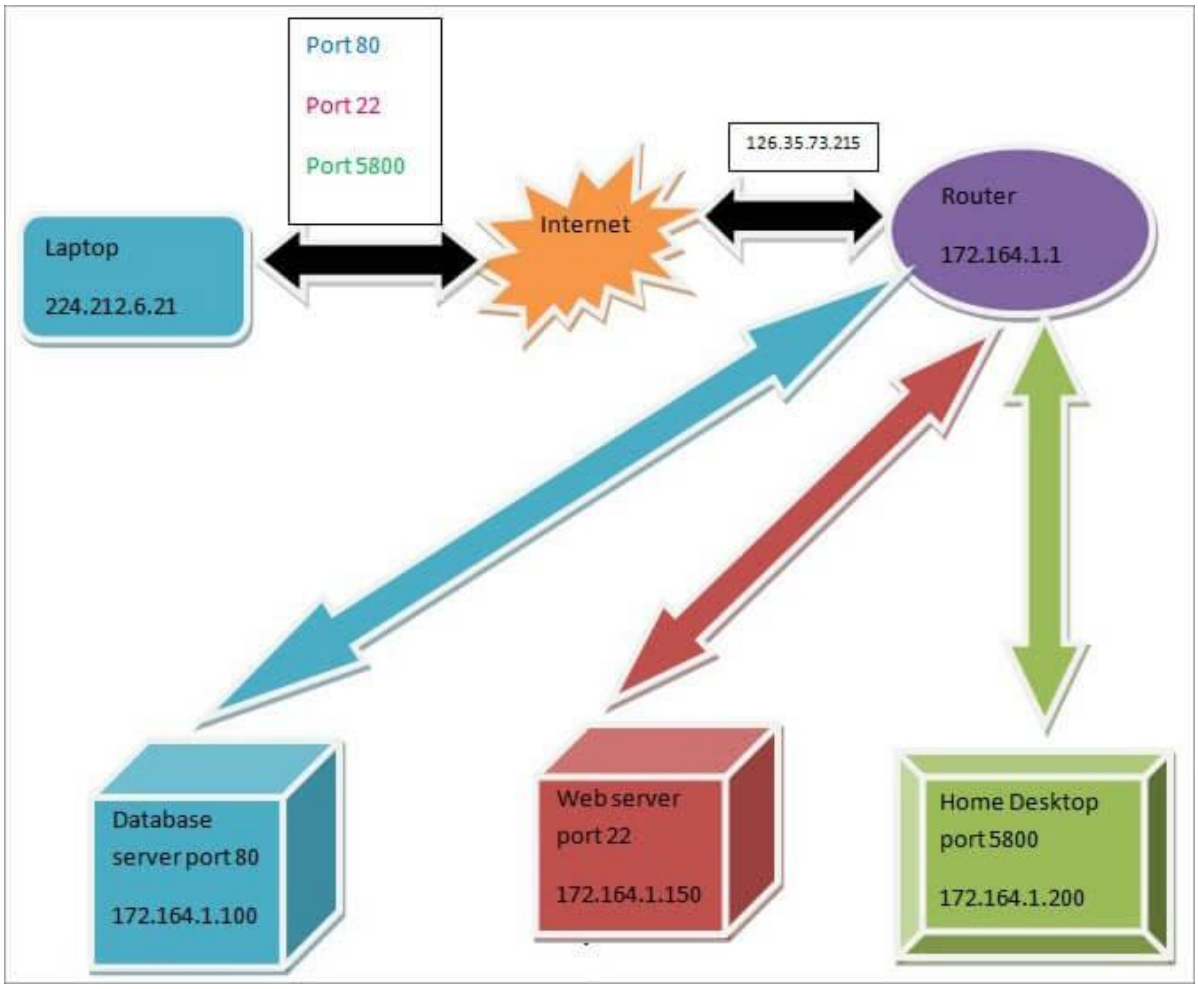
3. Dynamic Port Forwarding

To enable traffic to pass past a firewall or NAT on-demand, dynamic port forwarding exploits firewall pinholes. Clients are allowed to establish a secure connection with a dependable server that serves as a bridge between clients and several destination servers.

Dynamic port forwarding causes the user's SSH client to act as a SOCKS proxy server. An internet connection can be requested by applications using a proxy server thanks to the widely used SOCKS protocol. For each software or application that uses a proxy server, users must configure it separately, and when software is no longer using a proxy server, it needs to be reconfigured.

Port Forwarding Example





- As explained in the above diagram, by setting the forwarding rule on the home network, one can access the network even from the far end and the router will grant access to the right application with the right host computer.
- Suppose a person is outside home for some work and wants to access his home desktop and server, then he will make requests using different port numbers to his router. If he requests to grant access to the home network over port number 80, then the router will direct him to the database server having IP 172.164.1.100.
- When he sends a request over port number 22, then the router will route him to the webserver with IP 172.164.1.150 and if he wants to remotely control his home desktop, then the router will send him to IP 172.164.1.200 via port 5800.
- In this way, one can connect remotely to all the devices in the home network from outside the network if the port forwarding rule is set for the network on the router.

- In the rule, the combination of the specific port with the static IP address of the device is defined so that when needed to access, the router can grant access according to the pre-defined set of rules.