The system

The purpose of the Socks Proxy is to build a tunnel that allowing traffic to bypass Internet filtering to access content otherwise blocked by governments or workplaces. The client and server are connected through TCP. Each time when the client receives a TCP request, it will open a port and the server has a corresponding port, so the client and server communicate at layer 5 (session layer). All the TCP connections are transmitted between the corresponding port.

The server has the socket that is bound to a specific port number, and it just waits, listening to the socket for a client to make a connection request.

The client should know the hostname (address) of the server, and the corresponding port the server is listening. To make a connection request, the client tries to rendezvous with the server on the server's address and port. The client also needs to identify itself to the server so it binds to a local port number that it will use during this connection. Once the server accepts the connection, the server gets a new socket bound to the same local port and has its remote endpoint set to the address and port of the client. The new sockets ensure it can continue to listen to the original socket for connection requests while tending to the need of connected client. While for the client, if the connection is accepted, a socket is created and it will use the socket to communicate with the server.

To make it simple, will use a simple authentication method in socks5 - No authentication. But the connection between client and server are encrypted with Blowfish encryption algorithm. So the key is required at the start of connection.