VPN Code Documentation

Explanation of the code of a simple Virtual Private Network built using Java.

- Both the server and client use AES encryption to encrypt and decrypt messages. AES (Advanced Encryption Standard) is chosen for simplicity, but for real-world VPNs, you would use more advanced security and key management.
- The server and client simulate tunneling by sending encrypted messages over the TCP connection. Each message is prefixed with its length to ensure proper reading and writing of data.
- The `encrypt` and `decrypt` methods handle encryption and decryption using AES with a specified key (`AES_KEY`).
- The server waits for a client with a specific port number.
- The client looks for a server on a particular IP address that uses the matching port number. The client attempts to connect and the server accepts.
- The client sends a message, which is encrypted before sending to the server.
- The server decrypts the received message, processes it, and sends back a response, which is encrypted before sending back to the client.

This code lacks more secure key management, such as key exchange, and could use better authentication and error handling. Using established protocols like Transport Layer Security (TLS) would also be more secure than a simple AES encryption.