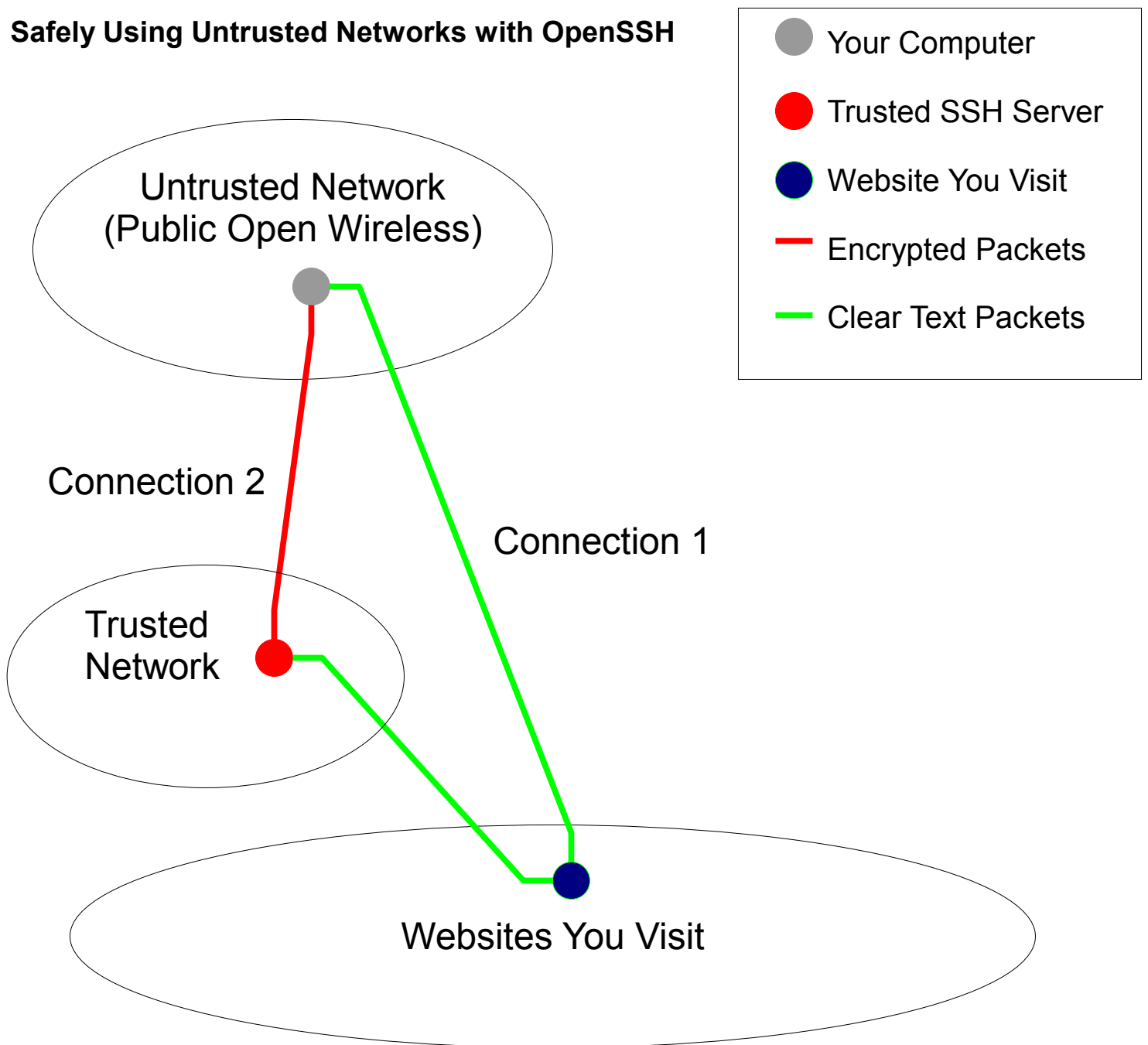


## Safely Using Untrusted Networks with OpenSSH



Connection 1 is an example of a normal Internet connection. Most people use this type of connection for browsing the Web. Where the line is green, the protocol (HTTP) does not encrypt data. On an untrusted network, others may be able to see the names of Web sites you visit and the data you send to and receive from the sites.

One way to stop this, is to connect to a trusted SSH server and forward HTTP connections through it. An example of that can be seen in Connection 2. Connect to the trusted SSH server like this:

```
ssh -N -D localhost:9999 user@trusted-ssh-server.com
```

Then, configure your Web browser to connect to a SOCKS5 proxy on 127.0.0.1 at port 9999. Finally, you want to ensure that all DNS queries go through the SSH server as well rather than the DNS resolvers on the untrusted network. In Firefox 3.5, for example, go to `about:config` and set `network.proxy.socks_remote_dns` to true. Now, the untrusted network cannot see your Web data or the names of the websites you visit.