

Most people know SSH as a tool for remote login, which it is, but it can be used in many other ways.

Create a SOCKS proxy to tunnel your web traffic (like when you're traveling)

```
ssh -D <port> <remote_host>
```

Set your web browser to use localhost:<port> as the proxy.

Connect to a Windows RDP host behind a bastion server

```
ssh -L <port>:<target_host>:3389 <bastion_server>
```

Set your RDP client to connect to localhost:<port>

Connect to your remote machine's VNC server without opening the VNC port

```
ssh -L 5901:localhost:5901 <remote_host>
```

Set your VNC client to connect to localhost:5901

You can follow this pattern with other ports you don't want to open to the world: LDAP (389), 631 (CUPS), 8080 (alternate HTTP), and so on.

Generate a new SSH key pair

```
ssh-keygen
```

Update the passphrase on an existing SSH key-pair

```
ssh-keygen -p
```

Copy a public SSH key to a remote host

```
ssh-copy-id -i <identity file> <remote_host>
```

SSH has a lot of command-line options, but if you use the same options for a host regularly, you can put an entry in the SSH configuration file (`~/.ssh/config`) instead. For example:

```
host myhouse
    User itsme
    HostName house.example.com
```

Then you can type `ssh myhouse` instead of `ssh itsme@house.example.com`.

Here are common command-line options and their configuration file equivalents. Some are simplified for common use cases. See the [ssh\(1\)](#) and [ssh\\_config\(5\)](#) manual pages for full details.

Command Line	Configuration File	Description
-l <login name>	User <login name>	The login name on the remote machine.
-i <identity file>	IdentityFile <identity file>	The identity file (SSH keypair) to use for authentication.
-p <remote port>	Port <remote port>	The port on which the remote SSH daemon is listening. (default: 22)
-C	Compression <yes no>	Compress traffic between hosts. (default: no)
-D <port>	DynamicForward <port>	Forward traffic on the local port to the remote machine.
-X	ForwardX11 <yes no>	Display X11 graphical programs from your remote host on the local host. (default: no)
-A	ForwardAgent <yes no>	Forward the authentication agent to the remote host. This is helpful if you'll then connect to a third host. (default: no)
-4 (use IPv4 only) -6 (use IPv6 only)	AddressFamily <any inet4 inet6>	Specify whether to use IPv4 or IPv6 only.
-L <local port>:<target host>:<target port>	LocalForward <local port>:<target host>:<target port>	Forward local traffic on the specified to port to the remote host and port.