OpenSSH Secure remote shell

CONCEPTS

Put per-host settings in ~/.ssh/config so a long command becomes just: ssh <alias>.

Client ssh + ssh-agent
↓ encrypted
Jump host optional bastion
↓ forwarded
Server sshd, authorized_keys

Keep the private key secret; only the .pub file ever leaves your machine.

CONNECT

ssh *<user>*@*<host>*
Log in to a host

ssh *<host>*
Log in as your local user name

ssh -p *<port>* *<user>*@*<host>*
Use a non-default port

ssh *<host>* *<command>*
Run a command and return

ssh -i *<keyfile>* *<host>*
Pick a specific private key

ssh -t *<host>* *<command>*
Force a terminal (sudo, top, tmux)

ssh -v *<host>*
Show debug output (up to -vvv)

ssh -o *<Option>*=*<value>* *<host>*
Set a config option for this run

ssh -C *<host>*
Compress the connection

KEYS

ssh-keygen -t ed25519 -C "*<comment>*"
Generate an Ed25519 key pair

ssh-keygen -t rsa -b 4096
Generate an RSA key (legacy servers)

ssh-copy-id *<user>*@*<host>*
Install your public key on a host

ssh-keygen -p -f *<keyfile>*
Change a key's passphrase

ssh-keygen -l -f *<keyfile>*
Show a key's fingerprint

ssh-keygen -R *<host>*
Forget a host in known_hosts

AGENT

eval "$(ssh-agent)"
Start an agent in this shell

ssh-add
Add the default key to the agent

ssh-add *<keyfile>*
Add a specific key

ssh-add -l
List loaded keys

ssh -A *<host>*
Forward your agent to the host

COPY FILES

scp *<file>* *<user>*@*<host>*:*<path>*
Upload a file

scp *<user>*@*<host>*:*<path>* *<dir>*
Download a file

scp -r *<dir>* *<host>*:*<path>*
Copy a directory

scp -P *<port>* *<file>* *<host>*:*<path>*
Use another port (capital P)

sftp *<user>*@*<host>*
Interactive file transfer session

TUNNELS

ssh -L *<lport>*:*<dest>*:*<dport>* *<host>*
Local forward: reach dest via host

ssh -R *<rport>*:*<dest>*:*<dport>* *<host>*
Remote forward: expose a local port on host

ssh -D *<port>* *<host>*
Open a local SOCKS proxy

ssh -N *<host>*
Forward only, run no command

ssh -f -N -L *<lport>*:*<dest>*:*<dport>* *<host>*
Tunnel in the background

ssh -J *<jump>* *<host>*
Connect through a jump host

CONFIG

ssh -G *<host>*
Print the effective settings

CONFIG (cont.)

Host *<alias>*
Start a config block

HostName *<name-or-ip>*
Real address of the alias

User *<user>*
Default login name

Port *<port>*
Default port

IdentityFile *<path>*
Key to use for this host

IdentitiesOnly yes
Offer only the listed key

ProxyJump *<jump>*
Always hop via this host

ServerAliveInterval 60
Send keepalives every 60 s

AddKeysToAgent yes
Auto-add keys on first use

Host *
Defaults for every host

MULTIPLEXING

ControlMaster auto
Share one connection per host

ControlPath ~/.ssh/cm-%r@%h:%p
Socket path for shared connections

ControlPersist 10m
Keep master alive after logout

ESCAPE KEYS

Enter ~.
Kill a hung session

Enter ~?
List escape sequences

RECIPES

Host entry with a jump host

```
# ~/.ssh/config
Host db
  HostName db.internal
  User deploy
  ProxyJump bastion
  IdentityFile ~/.ssh/id_ed25519
  ServerAliveInterval 60
```

First-time key login

```
ssh-keygen -t ed25519
ssh-copy-id <user>@<host>
ssh <user>@<host>
```