REFERENSI CEPAT SSH

Koneksi, key, konfigurasi, tunnel, SCP, SFTP

Koneksi

Koneksi Dasar

```
ssh user@host                  # connect to host
ssh -p 2222 user@host          # custom port
ssh user@host command           # run remote command
ssh -t user@host "top"         # force TTY allocation
```

Flag Koneksi

`-p port`	Koneksi ke port tertentu
`-i key`	Gunakan identity (private key) tertentu
`-t`	Paksa alokasi pseudo-terminal
`-v / -vv / -vvv`	Verbose debugging (semakin detail)
`-q`	Mode senyap (sembunyikan peringatan)
`-N`	Tanpa perintah remote (untuk tunnel)
`-f`	Jalankan di background sebelum perintah
`-J jump`	Jump host (ProxyJump)

Manajemen Key

Buat Key

```
ssh-keygen -t ed25519 -C "you@example.com"
ssh-keygen -t rsa -b 4096 -C "you@example.com"
ssh-keygen -t ed25519 -f ~/.ssh/mykey
ssh-keygen -p -f ~/.ssh/id_ed25519  # change passphrase
```

Deploy Public Key

```
ssh-copy-id user@host
ssh-copy-id -i ~/.ssh/mykey.pub user@host
# Manual: append .pub to remote authorized_keys
cat ~/.ssh/id_ed25519.pub | ssh user@host \
  "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

File Key

`~/.ssh/id_ed25519`	Private key (jaga kerahasiaannya)
`~/.ssh/id_ed25519.pub`	Public key (boleh dibagikan)
`~/.ssh/authorized_keys`	Remote: public key yang diterima
`~/.ssh/known_hosts`	Fingerprint host yang dikenal

File Konfigurasi

Dasar ~/.ssh/config

```
Host myserver
  HostName 192.168.1.100
  User deploy
  Port 2222
  IdentityFile ~/.ssh/deploy_key

# Then connect with just:
# ssh myserver
```

Opsi Konfigurasi Berguna

```
Host *
  ServerAliveInterval 60
  ServerAliveCountMax 3
  AddKeysToAgent yes
  IdentitiesOnly yes

Host bastion
  HostName bastion.example.com
  User admin
```

Direktif Konfigurasi

`Host`	Pola alias untuk entri
`HostName`	Hostname atau IP sebenarnya
`User`	Nama pengguna login
`Port`	Port remote (default 22)
`IdentityFile`	Path ke private key
`ProxyJump`	Lewati host lain sebagai perantara
`ServerAliveInterval`	Interval keep-alive (detik)
`IdentitiesOnly`	Hanya gunakan key yang ditentukan

Port Forwarding

Local Forwarding (-L)

```
# Access remote port 5432 via local port 5432
ssh -L 5432:localhost:5432 user@host
# Access remote-db:3306 through ssh host
ssh -L 3306:remote-db:3306 user@host
# Bind to all interfaces
ssh -L 0.0.0.0:8080:localhost:80 user@host
```

Remote Forwarding (-R)

```
# Expose local port 3000 on remote port 8080
ssh -R 8080:localhost:3000 user@host
# Allow remote connections from any interface
ssh -R 0.0.0.0:8080:localhost:3000 user@host
```

Dynamic Forwarding (-D)

```
# SOCKS5 proxy on local port 1080
ssh -D 1080 user@host
# Background SOCKS proxy
ssh -D 1080 -fN user@host
```

SCP & SFTP

SCP (Salinan Aman)

```
scp file.txt user@host:/remote/path/
scp user@host:/remote/file.txt ./local/
scp -r dir/ user@host:/remote/path/
scp -P 2222 file.txt user@host:/path/
```

SFTP (Transfer Interaktif)

```
sftp user@host
# Inside sftp session:
# put local.txt    — upload file
# get remote.txt   — download file
# ls / lcd / cd    — list / change directory
```

Flag Transfer

`-r`	Rekursif (salin direktori)
`-P port`	Tentukan port (SCP pakai -P, bukan -p)
`-C`	Aktifkan kompresi
`-l limit`	Batas bandwidth dalam Kbit/s
`-i key`	Gunakan identity file tertentu

Agent Forwarding

SSH Agent

```
eval "$(ssh-agent -s)"          # start agent
ssh-add ~/.ssh/id_ed25519       # add key to agent
ssh-add -l                      # list loaded keys
ssh-add -D                      # remove all keys
```

Meneruskan Agent

```
ssh -A user@host                # forward agent
# Or in ~/.ssh/config:
# Host myserver
#   ForwardAgent yes
```

Catatan Agent

Agent forwarding memungkinkan host remote menggunakan key lokal tanpa menyalinnya. Gunakan hanya pada host yang tepercaya. Lebih baik gunakan ProxyJump daripada agent forwarding bila memungkinkan.

Tunnel

Tunnel Persisten

```
# Background tunnel that stays open
ssh -fNT -L 5432:localhost:5432 user@host
# Auto-reconnecting tunnel (with autossh)
autossh -M 0 -fNT -L 5432:localhost:5432 user@host
```

Jump Host / Bastion

```
ssh -J bastion user@internal-host
ssh -J user1@hop1,user2@hop2 user@target
# Config equivalent:
# Host internal
#   HostName 10.0.0.5
#   ProxyJump bastion
```

Manajemen Tunnel

`-f`	Jalankan di background setelah autentikasi
`-N`	Tanpa perintah remote
`-T`	Nonaktifkan pseudo-terminal
`~.`	Matikan sesi SSH yang macet (escape)
`~C`	Buka command line untuk forwarding
`~#`	Tampilkan daftar koneksi yang diteruskan

Troubleshooting

Debug Koneksi

```
ssh -vvv user@host              # max verbosity
ssh -G user@host                # dump config (dry run)
ssh-keyscan host                # fetch host keys
ssh-keygen -R host              # remove from known_hosts
```

Masalah Umum

`Permission denied`	Key, user, atau izin ~/.ssh salah (700/600)
`Host key changed`	Jalankan ssh-keygen -R host, lalu sambungkan kembali
`Connection timed out`	Periksa firewall, port, dan keterjangkauan host
`Too many auth failures`	Gunakan -i untuk menentukan key atau IdentitiesOnly
`Broken pipe`	Tambahkan ServerAliveInterval ke konfigurasi

Izin File

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/id_ed25519     # private key
chmod 644 ~/.ssh/id_ed25519.pub # public key
chmod 600 ~/.ssh/authorized_keys
chmod 644 ~/.ssh/known_hosts
```

Praktik Keamanan Terbaik

Hardening Server

`PasswordAuthentication no`	Nonaktifkan login dengan password
`PermitRootLogin no`	Nonaktifkan akses SSH sebagai root
`AllowUsers deploy`	Whitelist pengguna yang diizinkan
`Port 2222`	Gunakan port non-default (hindari scanner)
`MaxAuthTries 3`	Batasi percobaan autentikasi

Praktik Key

Utamakan key Ed25519 (lebih kecil, lebih cepat, lebih aman).
Selalu atur passphrase pada private key.
Gunakan ssh-agent agar tidak perlu mengetik passphrase berulang.
Ganti key secara berkala; cabut key yang tidak digunakan.
Gunakan IdentitiesOnly untuk mengontrol key yang ditawarkan.

Multiplexing

Berbagi Koneksi

```
# In ~/.ssh/config
Host *
  ControlMaster auto
  ControlPath ~/.ssh/sockets/%r@%h-%p
  ControlPersist 600

# Create socket directory
mkdir -p ~/.ssh/sockets
```

Keuntungan Multiplexing

Menggunakan ulang satu koneksi TCP untuk beberapa sesi SSH ke host yang sama. Menghilangkan handshake berulang — koneksi lebih cepat dan overhead lebih rendah.
ControlPersist menjaga master tetap aktif (dalam detik).

Escape Sequence

Perintah Escape SSH

`~.`	Akhiri koneksi (matikan sesi yang macet)
`~^Z`	Suspensi sesi SSH
`~C`	Buka command line (tambah forwarding)
`~#`	Tampilkan daftar koneksi yang diteruskan
`~&`	Jalankan SSH di background (menunggu koneksi)
`~?`	Tampilkan bantuan escape
`~~`	Kirim tilde literal