

SSH

il coltellino svizzero del networking

COS'È SSH?

SSH (Secure Shell) è un protocollo di comunicazione sicura per l'accesso remoto a sistemi e il trasferimento di file. Nato negli anni '90 come sostituto sicuro di Telnet e rlogin, SSH utilizza la crittografia per proteggere i dati trasmessi tra client e server.

PERCHÉ SSH OGGI?

- Standard de-facto per l'amministrazione sicura
- Non solo shell: *porte, proxy, filesystem*
- Ovunque: Linux, macOS, Windows, container, router
- Ecosistema: Git, rsync, sftp, sshfs, Ansible

AUTENTICAZIONE

Basta password, benvenute **chiavi** e **agent**.

GENERAZIONE & INSTALLAZIONE CHIAVI

```
ssh-keygen -t ed25519 -C "giuseppe@linuxday" -f chiave_privata  
ssh-copy-id -i chiave_privata user@host
```

- Preferisci ed25519 (moderno, conciso)
- Proteggi con *passphrase*

AGENT: SBLOCCA LA CHIAVE UNA VOLTA SOLA

```
eval "$(ssh-agent -s)"  
ssh-add ~/.ssh/chiave_privata  
ssh user@host
```

- Evita di riscrivere passphrase ad ogni connessione
- Forward dell'agent per hop multipli (`ssh -A`, con cautela)

MINIMO HARDENING LATO SERVER

```
# /etc/ssh/sshd_config  
PasswordAuthentication no  
PubkeyAuthentication yes  
PermitRootLogin prohibit-password  
AllowUsers giuse deploy
```

Testa le chiavi prima di *spegnere* le password!

FORWARDING LOCAL (-L)

Porta locale → instradata verso un target remoto.

```
ssh -L 8080:webapp.internal:80 user@host  
# poi: curl -I http://localhost:8080
```

```
ssh -L 0.0.0.0:8080:webapp.internal:80 user@host  
# da altro host: curl -I http://192.168.1.100:8080
```


SICUREZZA & PRATICHE

- Limita l'esposizione a `localhost` quando possibile
- Chiudi la sessione quando non serve più

FORWARDING REMOTE (-R)

Porta remota sul bastion → inoltrata verso un target locale.

```
ssh -R 8080:webapp.local:80 user@host  
# richiede: AllowTcpForwarding yes su host
```

```
ssh -R 0.0.0.0:8080:webapp.local:80 user@host  
# richiede: GatewayPorts yes su host
```

ATTENZIONE

Esporre una porta su Internet è comodo, ma apre superfici d'attacco importanti: valuta attentamente i rischi.

- Bot e scanner cercano servizi esposti.
- Credenziali deboli o chiavi compromesse permettono compromessi diretti.
- Esposizione involontaria di dati sensibili.
- Se lasciata aperta, una porta rimane bersaglio finché non viene chiusa o monitorata.

DYNAMIC FORWARDING(-D)

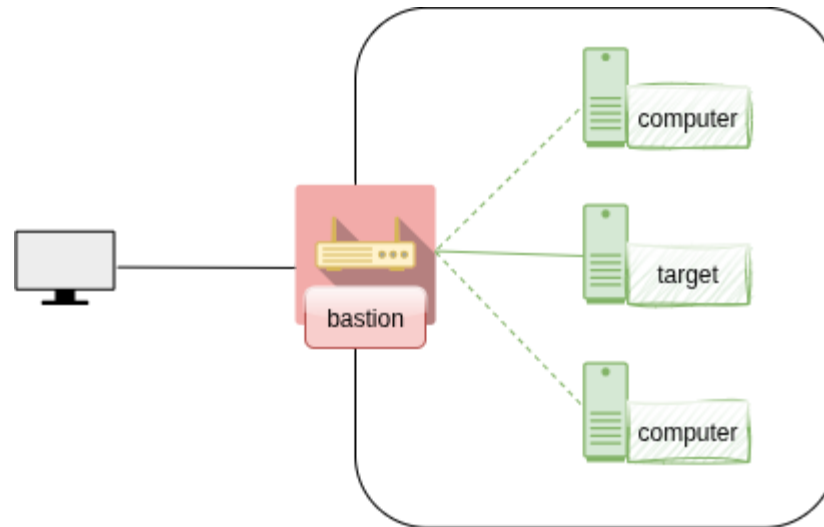
Proxy SOCKS “on-the-fly”: mini-VPN TCP stateless.

```
ssh -D 1080 demo@remote  
curl --socks5-hostname localhost:1080 https://ifconfig.me
```

QUANDO USARE -D

- Reti non fidate (hotel, guest)
- Testing di routing/geolocalizzazione
- Accesso a risorse TCP interne via bastion

JUMP HOST (-J)



```
ssh -J user@bastion user@target
```

CONFIG ELEGANTE CON ~ / .ssh/config & Include

Nomi amichevoli, default sensati, salti automatici.

ESEMPIO

```
1 Host bastion
2     HostName bastion.example.org
3     User giuse
4     Port 2222
5     IdentityFile ~/.ssh/id_ed25519
6
7 Host server1
8     HostName server1
9     User giuse
10    ProxyJump bastion
11
12 Include ~/.ssh/conf.d/*.conf
```


ESEMPIO

```
1 ssh bastion
```

MATCH (DIRETTIVE CONDIZIONALI)

Applica opzioni solo se la condizione corrisponde
(User, Group, Host, Address).

```
Match User deploy  
PasswordAuthentication no
```

MATCH (CONT)

Esegui qualsiasi comando, controllando il codice di uscita.

```
Match host internal-host !exec "/usr/bin/ping -c1 192.168.1.1"  
ProxyJump bastion.example.com
```

MULTIPLEXING

```
Host *  
  ControlMaster auto  
  ControlPath ~/.ssh/ctl-%r@%h:%p  
  ControlPersist 10m
```

Connessioni “istantanee” dopo la prima.

HARDENING & TROUBLESHOOTING

```
ssh -vvv server1  
ssh -G server1 | less
```

- Permessi stretti su `~/.ssh/*`
- Gestione `known_hosts` e collisioni

BONUS: DEVZAT — CHAT VIA SSH

- Devzat è un **server SSH** che porta in una chat invece della shell
- Identifica gli utenti tramite **chiave pubblica** (hash) • Admin via config

```
ssh tuo_nick@bucami.bglug.it -p 2222
```

Q&A

Domande, casi reali, dubbi?

licenziato sotto [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) 