Vše co jste chtěli vědět o SSH

... a báli jste se zeptat

(v kontextu správy serveru)

Prezentuje
Jakub Jelen
VPSFree.cz, Red Hat

Obsah

1. PKCS#11
2. Port Forwarding
    a. Local, Remote, Dynamic
3. Proxy
    a. SOCKS, VPN
4. Ostatní
    a. SSHFS, SSHFP

PKCS#11

PKCS#11

- API pro kryptografii s veřejným klíčem
- Kryptografické tokeny
  - HSM, TPM, SmartCard, Yubikey NEO, eID
- Bezpečnost: 2FA
  - Privátní klíč pouze na tokenu bez možnosti ukradení
  - Chráněný PIN, automatické zablokování
- Pro serverové i uživatelské klíče

PKCS#11

- Tvorba klíčů závislá na tokenu/ovladači [3]

```
$ LIB=/usr/lib/x86_64-*/opensc-pkcs11.so
$ LIB=/usr/lib64/opensc-pkcs11.so
```

- Získání veřejného klíče

```
$ ssh-keygen -D $LIB
```

- Připojení

```
$ ssh -I $LIB user@remotehost
```

- SSH-Agent (také pro server!)

```
$ eval `ssh-agent` && ssh-add -s $LIB
```

(odstranit původní klíče a restartovat server)

Port Forwarding

Lokální

- Lokální port → Existující port na serveru
  - Zpřístupnění vzdálené služby (šifrovaně)
  - Vyhnutí se firewallu / filtru obsahu ISP
- Př: Připojení na vzdálený mysql server

```
$ ssh -L 3306:localhost:3306 mysql
$ mysql -hlocalhost -P3306 --protocol=TCP -p
```

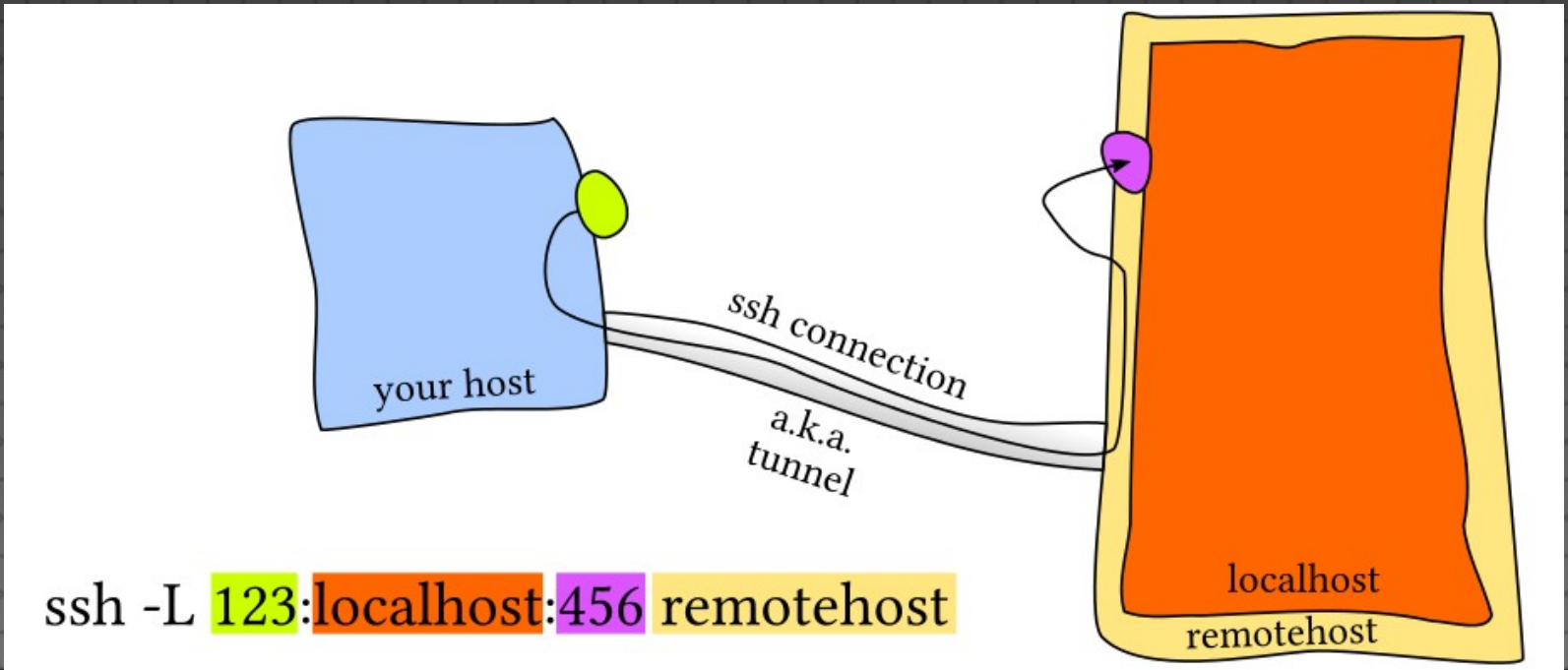
- Config: `LocalForward`

Lokální (příklad)

- Připojení na vzdálený HTTP server

```
$ ssh -L 8080:localhost:80 server
```

  - Firefox: http://localhost:8080/phpmyadmin/
    - `# echo "127.0.0.1 server-fqdn" >> /etc/hosts`
    - Firefox: http://server-fqdn:8080/



Vzdálené

- Port na serveru => Existující lokální port
  - Zpřístupnění lokální služby ze serveru
  - Počítač za NATem, Firewallem, bez veřejné IP
- Př: Reverzní tunel pro přístup do vnitřní sítě

```
[local]  $ ssh -R 2222:localhost:22 public
[public] $ ssh -p 2222 localhost
```

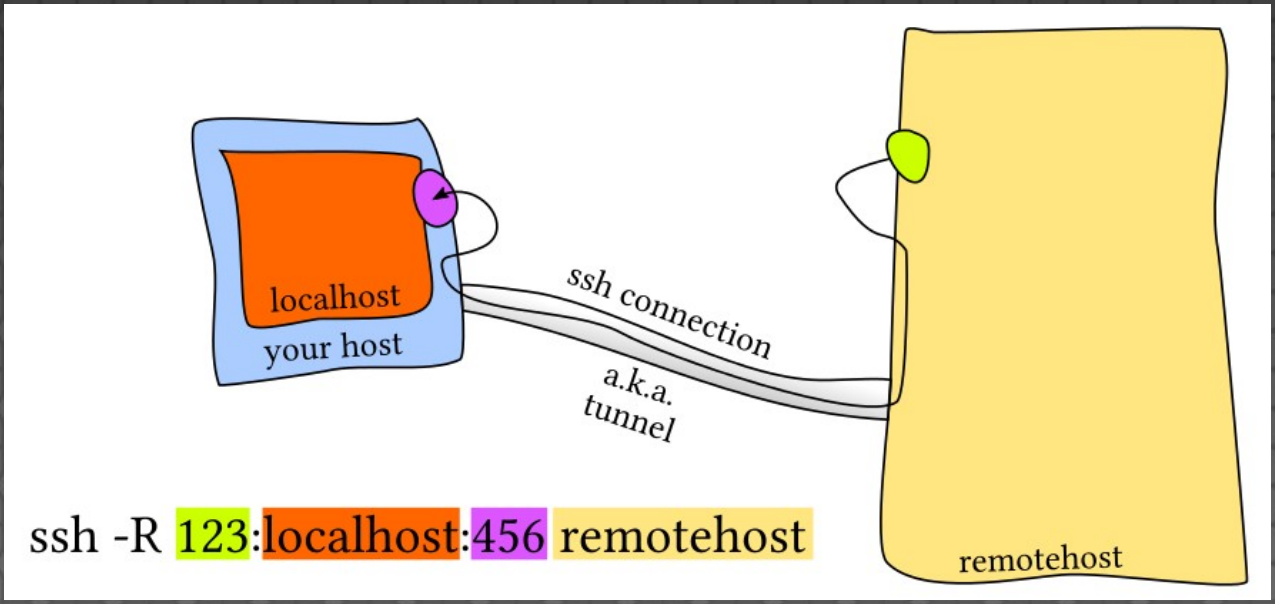
- Config: `RemoteForward`

Vzdálené (příklad)

- Tunel na kopírování souborů zpět:

```
[local]  $ ssh -R 2222:localhost:22 remote
```

- `[remote] $ scp file localhost:file -P 2222`



Port Forwarding obecně

- UNIX domain sockets (openssh-6.7)

```
$ S=/var/run/mysqld/mysqld.sock
$ ssh -R $S:$S -R 127.0.0.1:3306:$S mysql
```

- Povolení: `[all|local|remote|no]`
  - `AllowTCPForwarding`
  - `AllowStreamLocalForwarding`
- Adresa volného portu
  - Výchozí loopback (`127.0.0.1`)
  - Klient: `-g`
  - Server: `GatewayPorts`

Port Forwarding obecně

- Sdílení jediného spojení
  - `ControlMaster auto`
  - `ControlPath ~/.ssh/control-%l.%r@%h:%p`
  - `ControlPersist 2m`
- Pouze Port forwarding

```
$ ssh -NTfD localhost:9999 remote
```

  - `-N # no command`
  - `-T # no TTY`
  - `-f # background before command execution`

Dynamické

- SOCKS proxy
- Přesměrování TCP/IP provozu přes server
- Podpora IPv6, „Anonymizace“
- Obcházení pravidel ISP
- Př:

```
$ ssh -D localhost:9999 remote
```

  - Firefox: Nastavení → Pokročilé → Síť → Připojení → SOCKS host: 127.0.0.1, port: 9999
  - whatismyip.com

Proxy

SOCKS

= Dynamic Port Forwarding

- Rozdíl?

```
$ ssh -D localhost:9999 remote
```

  - Pouze tento počítač

```
$ ssh -D 147.32.77.220:9999 remote
```

  - Kdokoliv z lokální sítě

VPN

- `NetworkManager-ssh-gnome [4], sshuttle [5]`
- Ručně:
  - `Klient:`

    ```
    # ssh -w 0:0 remote
    ```

  - Server:
    - `PermitRootLogin [yes|without-password]`
    - `PermitTunnel [yes|point-to-point]`
  - Pokud více než p2p:
    - `# echo 1 | /proc/sys/net/ipv4/ip_forward`
    - Nastavení sítě

Ostatní

- SSHFS: FUSE + SFTP
  - `# sshfs hostname:/var/www /mnt/vps`
- SSHFP: DNS + hostkey fingerprint

```
$ ssh-keygen -r hostname -g
hostname IN TYPE44 \# 22 01 01
33aad4d544e85c8a8264471da2ce9ec85de86933
```

  - ssh_config: `VerifyHostKeyDNS`
- HostKey rotation: Pravidelná výměna klíčů
  - Klient ukládá všechny serverové klíče

Shrnutí

- Kniha „SSH Mastery”
- Yubikey: bezpečný klíč
- Lokální x Vzdálené přesměrování
- Obcházení omezení pomocí SOCKS proxy
- Ano, umíme také VPN

Otázky?

Kontakt:
jakuje@gmail.com

Zdroje a odkazy

- [0] SSH Mastery, J.W.Lucas, 2012
- [1] http://blather.michaelwlucas.com/archives/1132
- [2] http://unix.stackexchange.com/a/115906/121504
- [3] https://developers.yubico.com/yubico-piv-tool/SSH_with_PIV_and_PKCS11.html
- [4] https://github.com/danfruehauf/NetworkManager-ssh
- [5] https://github.com/apenwarr/sshuttle