

OpenSSH - einfach, sicher, verstehen

André Niemann, becon GmbH
vorname.nachname@becon.de

Tübix 2018



Über mich



- » System Engineer
- » WebPKI, Orchestrierung, Monitoring, SSH
- » bei der becon GmbH



- » Gründung in 1988 aus dem Konzernumfeld heraus
- » Standorte in München, Berlin und Fulda
- » Dienstleister für integrierte Data Center Services auf Konzern Niveau
- » Kunden wie Atos, Bosch, Linde, Nokia, Siemens, T-Systems, Wincor
- » GmbH in privater Hand mit starker Finanzkraft
- » International tätig, ISO 9001:2008 zertifiziert
- » Inkubator für Startups und Open Source Projekte
- » Mitbegründer der sys4 AG



SSH-einfach, sicher, verstehen

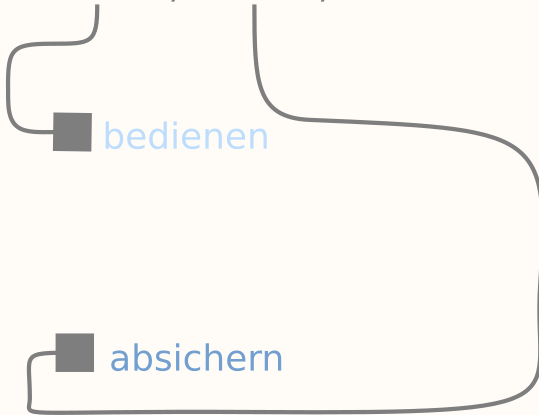


SSH-einfach, sicher, verstehen



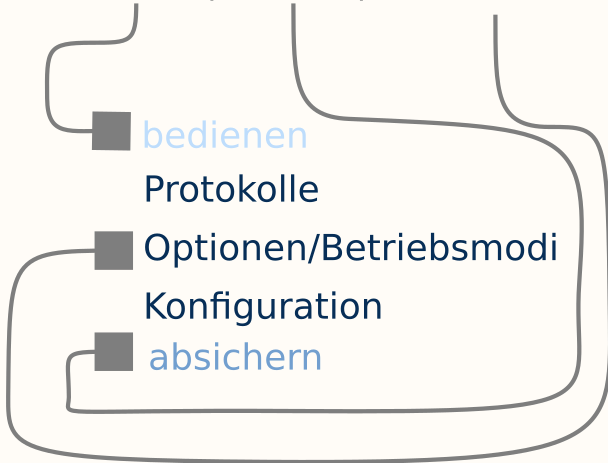


SSH-einfach, sicher, verstehen





SSH-einfach, sicher, verstehen



Warum SSH?



```
1 | o
2 | ---[]          -----
3 | |             | - -      °° |
4 | / \          | - -      |
5 |             -----
6 | \^-- du(+ Gerät)    \^-- Server
7 |
8 | o      o      o      o
9 | ---  ---  ---  ---
10 | |      |      |      |
11 | / \    / \    / \    / \
12 | \^-- andere (gucken zu)
```

(Was gefällt euch an) OpenSSH?

“das es klappt, es geht halt”

— OpenSSH User, IRC

(Was gefällt euch an) OpenSSH?

“das es klappt, es geht halt”

— OpenSSH User, IRC

“-NL ist die Magic, die man immer braucht ”

— another OpenSSH User, IRC

(Was gefällt euch an) OpenSSH?

“das es klappt, es geht halt”

— OpenSSH User, IRC

“-NL ist die Magic, die man immer braucht ”

— another OpenSSH User, IRC

“SSH funktioniert einfach(, nicht wie TLS)”

— bei ner Limo

Alle mögens, aber wer versteht es



Geht einfach.



alle mögens



geringer Konfigurationsaufwand - OOTB



weitreichende Konfigurationsmöglichkeiten



aber wie funktioniert es?



aber wie konfigurier ich es(besser)?

Was ist (Open)SSH?



Recap

- » OpenSSH - wohl populärste SSH-2 Implementierung
- » IETF RFC 4251-54
- » Secure remote shell + (secure) Transportlayer Tunneling
- » andere: Dropbear, proprietär, ..
- » Client (OpenSSH, Dropbear, Putty)
- » Server (OpenSSH; Dropbear)

SSH vs TLS



SSH

- » built-in PFS
- » Tofu, (priv) CA optional(2006)
- » modul. Ciphersupport
- » mehrere Protokolle, erweiterbar
- » beidseitig Authentisiert(Key, Host based, pass)

TLS

- » PFS optional
- » (public) CA-Trustmodel
- » modul. Ciphersupport
- » ebenfalls Modular
- » beidseitig nur mit Client-Cert

Entfernt anmelden



» ssh user@host

Entfernt anmelden



» ssh user@host

☹ Password, wie doof.



- » `ssh user@host`
- ☹ Password, wie doof.
- » `ssh-keygen`
- » `ssh-copy-id || cat`
`.ssh/authorized_keys < id.pub`
- » `ssh user@host [-i id.pub]`

Entfernt anmelden



- » ssh user@host
- ☹ Password, wie doof.
- » ssh-keygen
- » ssh-copy-id || cat
.ssh/authorized_keys < id.pub
- » ssh user@host [-i id.pub]
- ☹ immernoch Password, wie doof.



» eval gpg-agent



- » eval gpg-agent
- » ssh-add



- » eval gpg-agent
- » ssh-add
- » ssh-add -l



- » `eval gpg-agent`
- » `ssh-add`
- » `ssh-add -l`
- » `ssh user@host`



- » eval gpg-agent
- » ssh-add
- » ssh-add -l
- » ssh user@host
- 😊 Nice! Geht da mehr?



» ssh -A host



- » `ssh -A host`
- » `env | grep -i auth`
- » `SSH_AUTH_SOCK=/tmp/ssh-T0IBsSoXjW/agent.5686`



- » `ssh -A host`
- » `env | grep -i auth`
- » `SSH_AUTH_SOCK=/tmp/ssh-T0IBsSoXjW/agent.5686`
- » `ssh otherhost`



» ssh [-v] user@host

» ~ + .

» ~ +  + 

» ~ + .

» ssh host 'uname -a'



» ssh [-v] user@host

» ~ + .

» ~ +  + 

» ssh host 'uname -a'

OpenSSH - Protokolle



- » Transportlayer Proto
- » Authentication Proto
- » Connection Proto

OpenSSH - Protokollüberblick

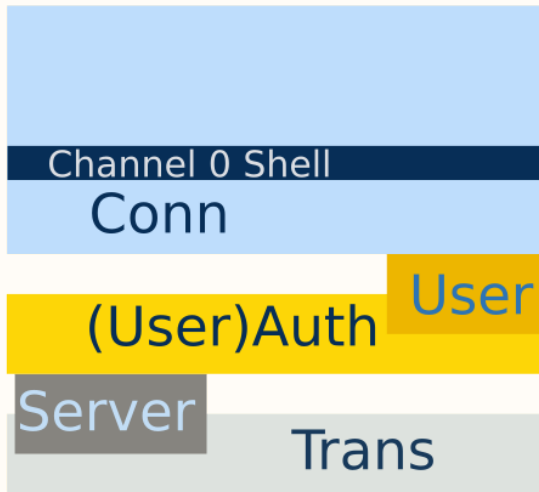
Server

Trans

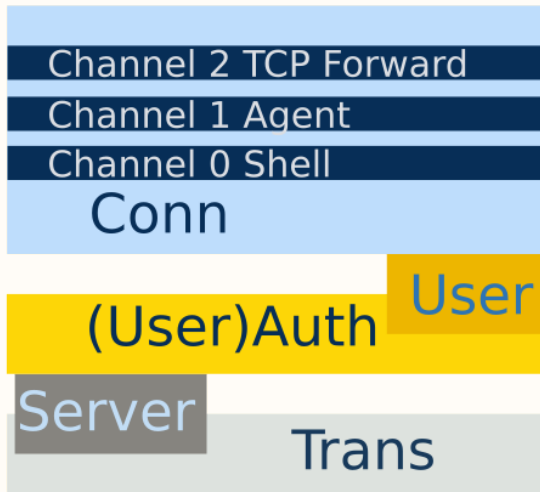
OpenSSH - Protokollüberblick



OpenSSH - Protokollüberblick



OpenSSH - Protokollüberblick



The Secure Shell (SSH) Transport

Transport Layer

This document describes the SSH transport layer protocol, which typically runs on top of TCP/IP. The protocol can be used as a basis for a number of secure network services. It provides strong encryption, server authentication, and integrity protection. It may also provide compression.

The Secure Shell (SSH) Authent

Authentication Protocol

The Secure Shell Protocol (SSH) is a protocol for secure remote login and other secure network services over an insecure network. .. The SSH authentication protocol runs on top of the SSH transport layer protocol and provides a single authenticated tunnel for the SSH connection protocol.

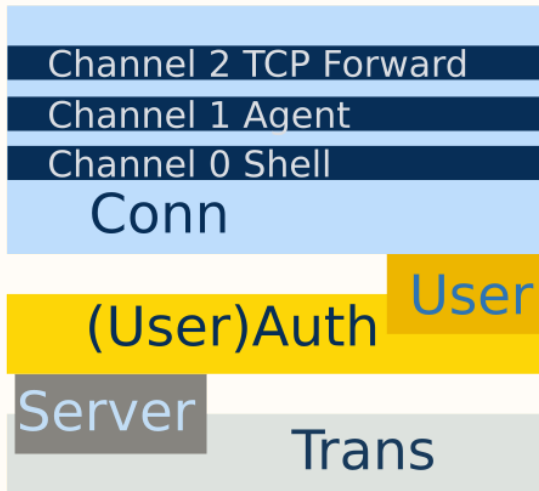
SSH Connection Protocol



Connection Protocol

This document describes the SSH Connection Protocol. It provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. All of these channels are multiplexed into a single encrypted tunnel.

OpenSSH - Protokollüberblick



Live!





» ssh [-v] user@host

» ~ + .

» ~ +  + 

» ssh host 'uname -a'



» ssh-agent

» gpg-agent

```
1 | $ env | grep -i auth
2 | SSH_AUTH_SOCK=/tmp/ssh-srFyhRtSTS3V/agent.2185
3 |
4 | agent-security:
5 | andre@skyfog:~/talks/ssh-mini$ ls -l /tmp/ssh-
   | srFyhRtSTS3V/agent.2185
6 | srw----- 1 andre andre 0 May 23 15:23 /tmp/ssh-
   | srFyhRtSTS3V/agent.2185
```

» ssh-add -c key

» -l

» -D / -d key

» -x (to lock)

Client Konfigurationen



```
man 5 ssh_config
```



```
man 5 ssh_config
```

- » command-line options
- » `/.ssh/config`
- » `/etc/ssh/ssh_config`

/.ssh/config



```
1 Host *
2     KexAlgorithms curve25519-sha256@libssh.org,diffie-
3     hellman-group-exchange-sha256
4     Ciphers chacha20-poly1305@openssh.com, aes256-
5     gcm@openssh.com
6
7 Host localhost
8     VisualHostKey yes
9     Identityfile legacyKey
10
11 Host Jump.box
12     User andre
13     ForwardAgent yes
14     Port 4242
```

Key Authentication



```
man 1 ssh-keygen
```

- » id_rsa
- » id_dsa
- » id_ecdsa
- » id_ed25519
- » id_??-cert ?



- » 'local Database' (/.ssh/known_hosts)
- » Textfile (/.ssh/known_hosts2)
- » SSHFP Records
- » SSH CA -> (AUTHORIZED_KEYS FILE FORMAT section)
- » UpdateHostKeys

SSH Key signing/CA



- » `ssh-keygen -f ssh-ca -b 4096`
- » `echo "cert-authority $(cat ssh-ca.pub)" » ~/.ssh/authorized_keys`
- » `ssh-keygen -s signing-key -l key-identifier -h -n hostname -V +52w host-key`

siehe `/etc/ssh/sshd_config`

- » SSH Version
- » Rootlogin
- » AllowUsers/Groups
- » ..

zusätzliche Sicherheitsfeatures

- » privilege Separation
- » rekeying
- » erweiterbarer Chiffrensupport

Ansätze zur Härtung



- » keine CBC, RC4 Cipher
- » keine alten Hash-Algos (< sha256)
- » kein pass-auth
- » private Schlüssel schützen.
- » \geq rsa2048



- » keine CBC, RC4 Cipher
- » keine alten Hash-Algos (< sha256)
- » kein pass-auth
- » private Schlüssel schützen.
- » \geq rsa2048

- » bettercrypto.org
- » mozilla wiki (
 <https://wiki.mozilla.org/Security/Guidelines/OpenSSH>)
- » BSI TR-02102-4
- » Vorschläge für aktuelle?

Check it



Secure | <https://sshcheck.com/server/github.com/22>

Rebex SSH Check

Rebex SSH Test result for github.com:22

General information

Server Identification:	SSH-2.0-libssh_0.7.0
IP Address:	192.30.255.113
Generated at:	2018-06-09 08:37:58 UTC (just now)

Key Exchange Algorithms

<code>diffie-hellman-group-exchange-sha256</code>	Diffie-Hellman with MODP Group Exchange with SHA-256 hash ⓘ	Secure
<code>curve25519-sha256@libssh.org</code>	Elliptic Curve Diffie-Hellman on Curve25519 with SHA-256 hash ⓘ	Secure
<code>ecdh-sha2-nistp256</code>	Elliptic Curve Diffie-Hellman on NIST P-256 curve with SHA-256 hash ⓘ <small>becoming obsolete</small>	Secure
<code>ecdh-sha2-nistp384</code>	Elliptic Curve Diffie-Hellman on NIST P-384 curve with SHA-384 hash ⓘ <small>becoming obsolete</small>	Secure
<code>ecdh-sha2-nistp521</code>	Elliptic Curve Diffie-Hellman on NIST P-521 curve with SHA-512 hash ⓘ <small>becoming obsolete</small>	Secure

Server Host Key Algorithms

<code>ssh-rsa</code>	RSA with SHA-1 hash ⓘ <small>SHA-1 is becoming obsolete.</small>	Secure
<code>ssh-dss</code>	NIST Digital Signature Algorithm (DSA) with SHA-1 hash ⓘ	Not Secure

Tunneling



- » `ssh -NL 9002:weistmeineip.de:80 andre@example.net`
- » `ssh -NR *:50020:localhost:22 example.net`
- » `ssh example.net -p 1337 -ND 33333`



» ssh -NL 9000:target:88888 andre@jumphost



- » `ssh -NL 9000:target:88888 andre@jumphost`
- » `forwards localhost:9000 zu target:8888`

Reverse



» `ssh -R 8080:localhost:22 andre@reversehost`

Reverse



- » `ssh -R 8080:localhost:22 andre@reversehost`
- » einkommend auf reversehost:8080 geht an localhost:22

Dynamic



» ssh -ND 33334 andre@jumphost

Dynamic



- » `ssh -ND 33334 andre@jumphost`
- » Webbrowser -> Socks

Dynamic



- » `ssh -ND 33334 andre@jumphost`
- » Webbrowser -> Socks
- » `localhost:33334`

Dynamic



- » `ssh -ND 33334 andre@jumphost`
- » Webbrowser -> Socks
- » `localhost:33334`
- » `http://weistmeineip.de` -> IP von jumphost

Jump Host



```
1 # First jumphost. Directly reachable
2 Host alphajump
3   HostName jumphost1.example.org
4
5 # Host to jump to via jumphost1.example.org
6 Host behindalpha
7   HostName behindalpha.example.org
8   ProxyCommand ssh alphajump netcat -w 120 \%h \%p
```

```
1 # First jumphost. Directly reachable
2 Host betajump
3   HostName jumphost1.example.org
4
5 # Host to jump to via jumphost1.example.org
6 Host behindbeta
7   HostName behindbeta.example.org
8   ProxyJump betajump
```

Channel Multiplexing



```
1 | Host machine1
2 |     HostName machine1.example.org
3 |     ControlPath ~/.ssh/controlmasters/%C
4 |     ControlMaster auto
5 |     ControlPersist 10m

1| ssh (-M) -S /home/andre/.ssh/control@mp example.host
```

Pubkey + 2FA



```
1|AuthenticationMethods publickey,password
```

```
1|local ~ \ $ ssh root@box  
2|Authenticated with partial success.  
3|root@box's password:  
4|Welcome to box
```

siehe <https://www.privacyidea.org/ssh-keys-and-otp-really-strong-two-factor-authentication/>

- » mosh
- » sshfs(automounter)
- » rsync
- » SFTP(mit Keys)
- » SCP
- » ...


weitere Optionen



- » TunnelDevice
- » commands whitelist
- » restricted shells
- » fail2ban
- » SSH auth_command
- » ssh-agent
- » AutoSSH
- » sshlh



Was ist noch zu tun?



-  mehr über eure Infrastrukturtools reden!

Was ist noch zu tun?



-  mehr über eure Infrastrukturtools reden!
-  alle Jahre mal Configs reviewen

Was ist noch zu tun?



- 👤 mehr über eure Infrastrukturtools reden!
- ⚙️ alle Jahre mal Configs reviewen
- 🔒 mit Ciphern ebenso.





- » Siehe Cookbooks (unten)
<https://en.wikibooks.org/wiki/OpenSSH/Overview>
- » die Distro Wikis.
- » SSH manpages

Weiterhin Wissenvermittlungsdurs

- » Tolle Themen im Angebot?
- » Tolle Vorträge in Berlin?
- » Tolles Thema(mit Vortragendem) zu vermitteln?
- » Tolles Publikum jeden ersten Donnerstag des Monats

Weiterhin Wissenvermittlungsdurs

- » Tolle Themen im Angebot?
- » Tolle Vorträge in Berlin?
- » Tolles Thema(mit Vortragendem) zu vermitteln?
- » Tolles Publikum jeden ersten Donnerstag des Monats
- » kontakt@flarp.de