

Uebersicht

- SSH & screen?
- SSH Basic
- SSH Key Generierung
- SSH Key Management
- SSH Port Forwading
- SSH scp/sftp
- screen

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH & screen?

SSH?

- Protokoll / Programm
- Verschlüsselung
- Authentifizierung
- Integrität

screen?

- 'tabbed windowing'
- &bissl mehr

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - Basics

- **ssh** (openSSH client)
- **ssh-keygen** (Generierung von Schluessel)
- **ssh-agent** (Agent zur Authentifizierung)
- **ssh-add** (hinzufuegen von Ids an Agent)
- **ssh-argv0** (ersetzt ssh durch hostname)
- **scp** (kopiert Files)
- **sftp** (fuer sicheres FTP)

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - Basics

Aufbau einer Verbindung:

`ssh user@host`

z.B.: `$ssh john@example.com`

`ssh -p <port > user@host`

z.B.: `$ssh -p 1234 john@example.com`

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - KeyGen.

Key Generierung:

```
ssh-keygen -t <rsa1,rsa,dsa>
```

```
z.B.: $ssh-keygen -t rsa
```

```
ssh-keygen -t <type> -b <bit>
```

```
z.B.: $ssh-keygen -t rsa -b 2048
```

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - KeyGen.

~/Key Files: RSA1, RSA, DSA

~/.ssh/identity

~/.ssh/identity.pub

~/.ssh/id_rsa

~/.ssh/id_rsa.pub

~/.ssh/id_dsa

~/.ssh/id_dsa.pub

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - KeyGen

File: `~/.ssh/authorized_keys`

`~/.ssh/authorized_keys`: enthaelt pub Keys auf remote h.

```
local$ scp id_rsa.pub user@host:
```

```
remote$ cat id_rsa.pub >> ~/.ssh/authorized_keys
```

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - KeyManagement

ssh-agent: speichert key passphrase

falsch!: `$ ssh-agent`

richtig!: `$ eval `ssh-agent``

Vorteil: keine passphrase tippen
nur Signatur wird uebertragen

Nachteil: bei logout 'agent' verloren

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - KeyManagement

alternative: keychain

Vorteil: kein tippen der Passphrase

nur Key Signatur wird uebertragen

Passph. ist nach Logout noch da

Nachteil: bei kompromittierter Session, fuer Angreifer offen

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - KeyManagement

Files: ~/.ssh/config

```
# Beispiel
```

```
Host abel
```

```
Hostname 141.28.34.101
```

```
User koerner
```

```
Port 22
```

```
Protocol 2
```

Fuer Quickstart: In -s /usr/bin/ssh-argv0 abel

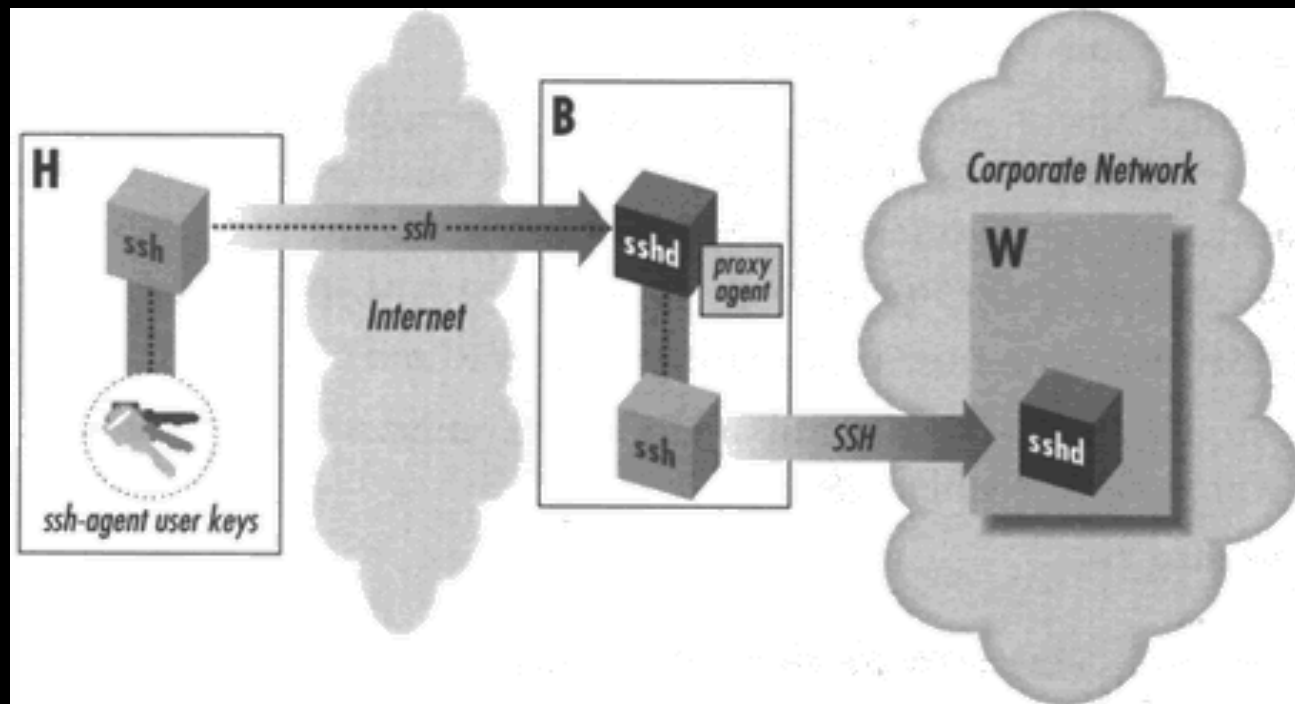
SSH/screen

SSH - KeyManagement

AgentForwarding:

“ForwardAgent yes” in ~/.ssh/config

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser



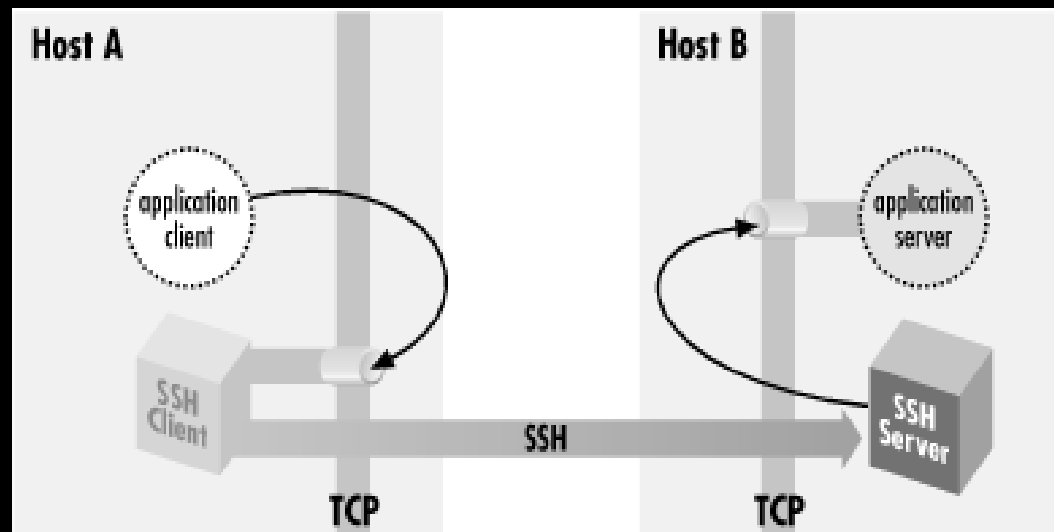
SSH/screen

SSH - Port Forwarding

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

-L(ocal)

\$ssh -L 2345:localhost:143 imap.mail.de



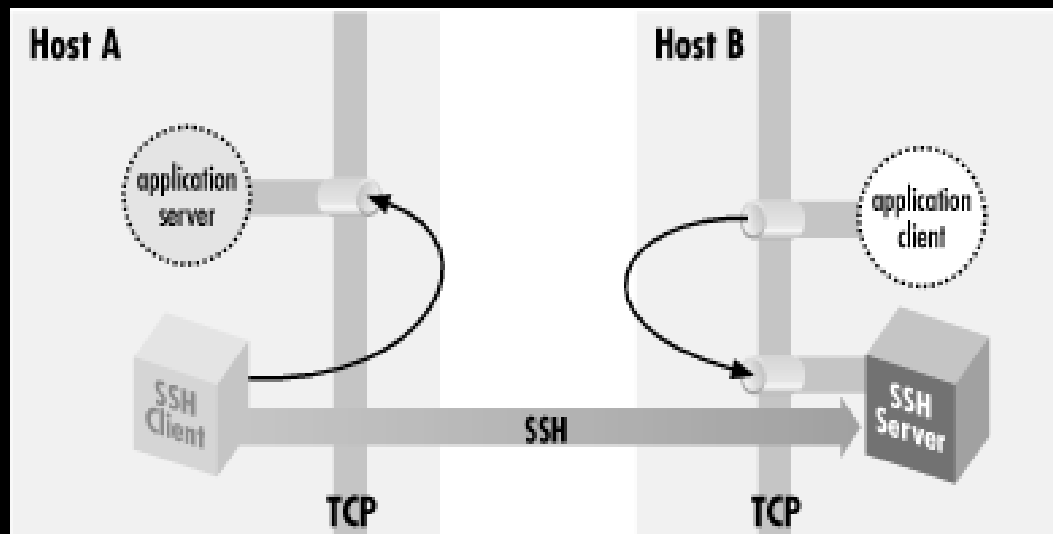
SSH/screen

SSH - Port Forwarding

-R(emote)

`$ssh -R 2345:localhost:143 client`

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser



SSH/screen

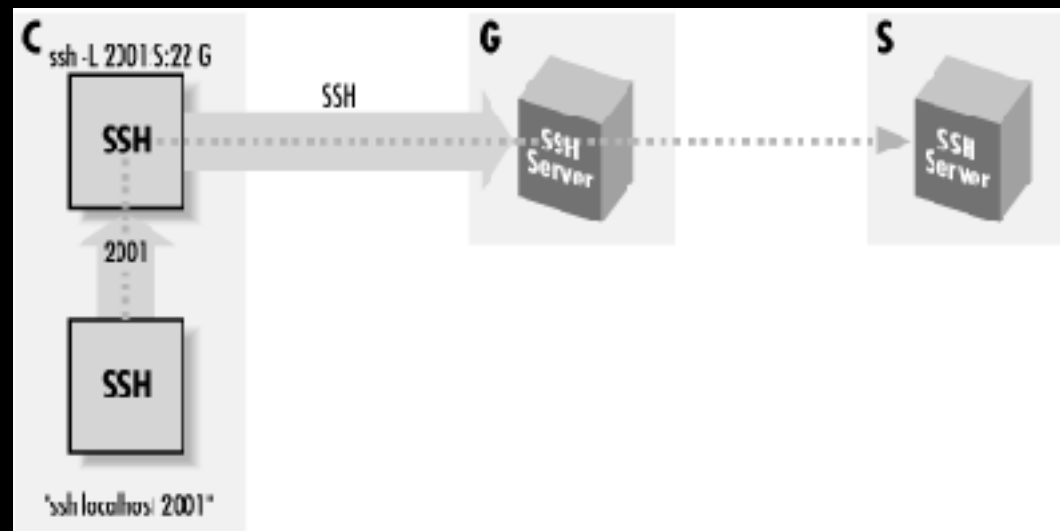
SSH - Port Forwarding

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH-in-SSH:

```
$ ssh -L 2001:S:22 G
```

```
$ ssh -P 54326 localhost
```



SSH/screen

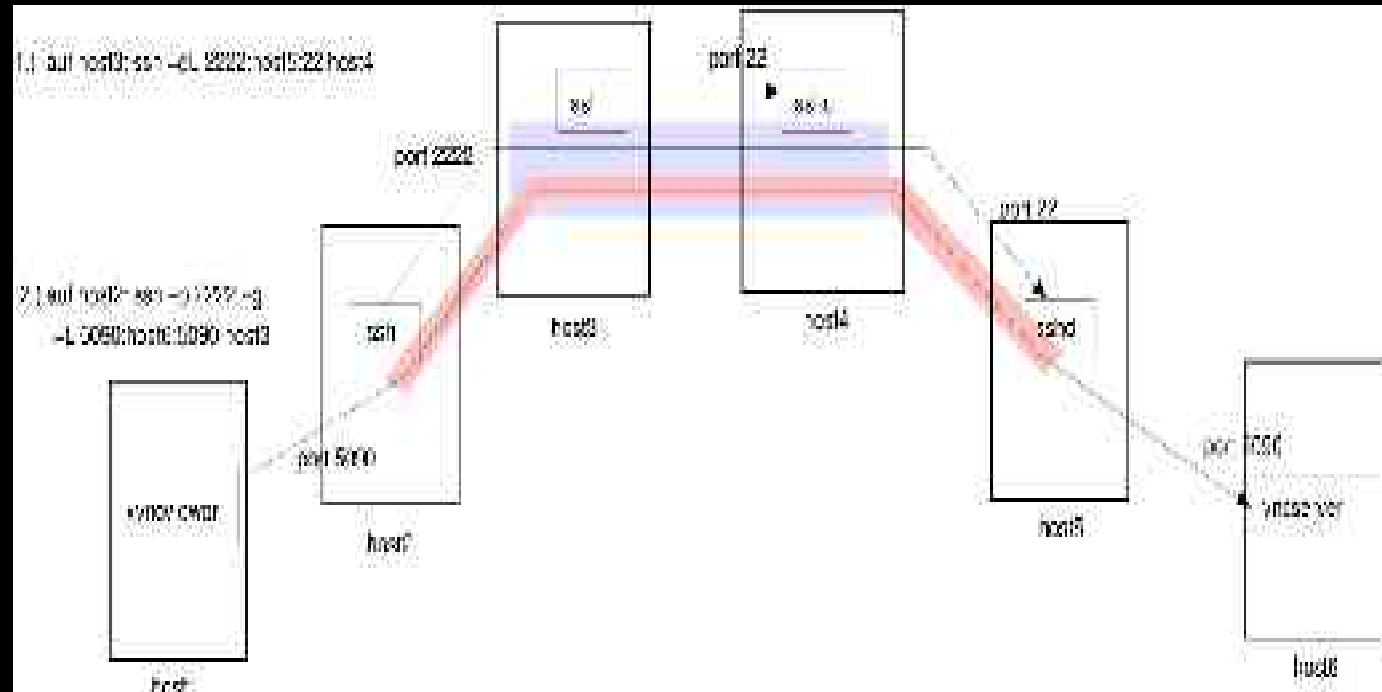
SSH - Port Forwarding

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH in SSH ... :

```
host3$ ssh -gL 2222:host5:22 host4
```

```
host2$ ssh -p 2222 -gL 5090:host6:5090 host5
```



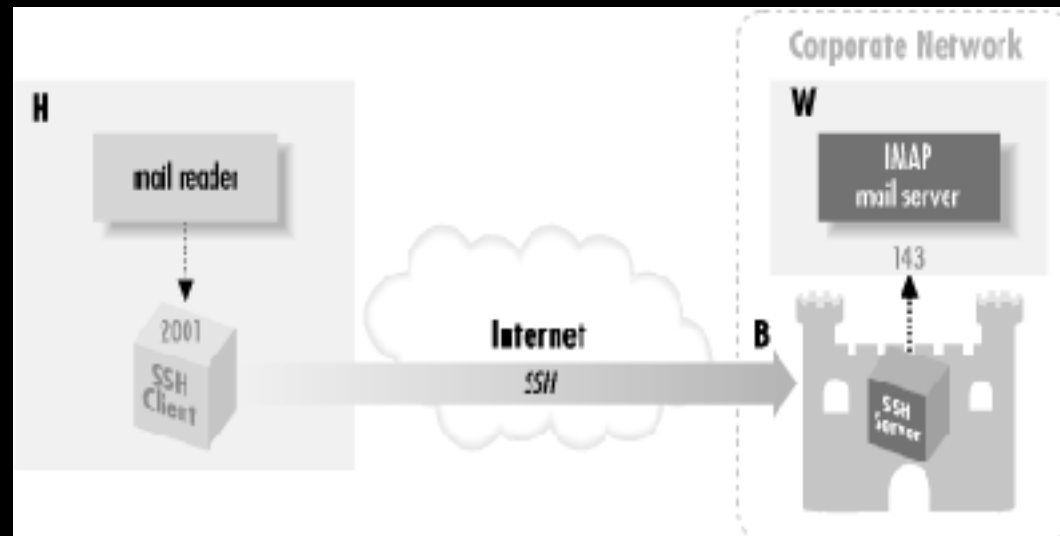
SSH/screen

SSH - Port Forwarding

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

Firewall umgehen:

```
$ ssh -L2001:W:143 B
```



SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - scp/sftp

scp/sftp:

scp user@host:file local

scp -r user@host:file local (rekursiv)

scp host:file .

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

SSH - scp/sftp

scp/sftp:

sftp user@host:file local

sftp -b file user@host

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

screen

`/etc/screenrc || ~/.screenrc`

default Keybindings:

C-a c neues Fenster

C-a C ~clear

C-a “ listet aktuelle Fenster

C-a h Logfile erzeugen

C-a A setzen vom Fenster Titel

C-a d abmelden von screen session

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

screen

`/etc/screenrc || ~/.screenrc`

default Keybindings:

C-a H "Screenshot"

C-a S splitten vom Fenster

C-a X schliessen von gesplitteten Fenster

C-a k schliessen von Fenster

C-a ? hilfe

C-a C-\ kill alle Fenster & beende screen

SSH/screen

- SSH & screen?
- SSH Basics
 - KeyGen.
 - KeyManagmnt.
- SSH Advanced
 - Port Forw.
 - scp/sftp
- screen
 - Keybindings
 - MultiUser

screen

Multi-User Mode:

```
user1$ screen -S test
```

```
in Screen "C-a :" -> multiuser on
```

```
in Screen "C-a :" -> addacl user2
```

```
user2 $ screen -r user1/test
```

SSH/screen

Quellen

- SSH & screen?

- SSH Basics

- KeyGen.

http://www.hn.edu.cn/book/NetWork/NetworkingBookshelf_2ndEd/ssh/index.htm

- KeyManagmnt.

http://infosecuritymag.techtarget.com/articles/june01/features_pr

- SSH Advanced

- Port Forw.

<http://www.jfranken.de/homepages/johannes/vortraege/ssh1.de.l>

- scp/sftp

<http://www.delorie.com/gnu/docs/screen/screen.html>

- screen

<http://www.michael-prokop.at/screen/index.php3>

- Keybindings

<http://nakedape.cc/wiki/ApplicationNotes/ScreenNotes>

- MultiUser

<http://www.openssh.org>

<http://www-106.ibm.com/developerworks/linux/library/l>

[-keyc3/?Opent=grl,l=929,p=Kp1](http://www-106.ibm.com/developerworks/linux/library/l-keyc3/?Opent=grl,l=929,p=Kp1)

O'reilly SSH Secure Shell: The Definitive Guide