

Workshop Rechnerbenutzung

Dennis Keitzel (6keitzel)

KunterBuntesSeminar
Wintersemester 2010

28. Oktober 2010

Inhalt des Seminars

- 1 Netzzugang
- 2 Zugriff auf das Rechenzentrum
- 3 Dateien übertragen
- 4 Drucken

Zugang via LAN oder WLAN

- LAN-Zugang über
 - Blau-markierte Dosen (z.B. D-202)
 - Fachschaftsräume in Haus E
- WLAN-Zugang über SSID
 - 'UHH' (unverschlüsselt)
 - 'UHH-WPA' (WPA2-Enterprise)
 - 'eduroam' oder '802.1X' identisch zu 'UHH-WPA'
- Authentifizierung über WPA2-Enterprise und/oder VPN

Authentifizierung via VPN (PPTP) [1]

Linux (Ubuntu)

- Konfiguration über den NetworkManager

Windows

- Konfiguration über die Systemsteuerung
- *Verbindung mit dem Arbeitsplatz herstellen*

Mac

- Konfiguration über die Systemeinstellungen
 - 'Netzwerk' → Im Menü: 'VPN' → Im Menü '+' → Anschluss: 'VPN' und VPN-Typ: 'PPTP' → 'Erstellen'

Authentifizierung via VPN (PPTP) [1]

- VPN-Server des RZ von überall aus erreichbar
- Host: `fbivpn.informatik.uni-hamburg.de` (134.100.5.65)
- Benutzername: RZ-Kennung (Bsp: `6keitzel`)
- Domäne: `INFORMATIK`
- Passwort: RZ-Passwort

Authentifizierung über Radius-Server [1]

Erfolgt implizit bei der Verwendung des 'UHH-WPA'-WLANs

Linux (Ubuntu)

- Über den NetworkManager
- Root-Zertifikat der Telekom erforderlich

Windows

- Supplicant-Software erforderlich (Enthält das Root-Zertifikat)
- Konfiguration über einen Wizard bei der Installation

Mac

- Ebenfalls Root-Zertifikat der Telekom erforderlich
- Konfiguration über die Netzwerkeinstellungen (Airport)

Authentifizierung über Radius-Server [2]

am Beispiel NetworkManager

- Sicherheit: WPA2 & WPA2 Enterprise
- Authentifizierung: Tunneled TLS
- Anonyme Identität: `anonymous@uni-hamburg.de`
- Innere Authentifizierung: PAP
- Benutzername: `<RRZ-Kennung>@uni-hamburg.de`
- Passwort: Das jeweilige Passwort

Bewertung: Informatik-VPN

Pro

- Internetzugang ohne Proxyserver
- Einfache Nutzung der Drucker des RZ
- Schnell
- **Echtes Internet ohne Restriktionen! (fast)**

Contra

- Schwergewichtig durch virtuelle Netzwerkkarte plus Tunnel
- Im Gegensatz zu UHH-WPA ein zusätzlicher Schritt
- Keine externen SMTP-Server erreichbar (Port 25)

Bewertung: Radius (WPA-Enterprise)

Pro

- Fast keine Portsperrungen
- Tlw. Schnell
- Nur ein Schritt
- eduroam

Contra

- HTTP/HTTPS gesperrt, Proxy ist Pflicht
 - Muss extra im Browser eingetragen werden
 - langsam
 - Aufzeichnungen?
- RRZ != RZ

Software für die kommenden Themen

- <https://mafiasi.de/workshop>

Das Werkzeug überhaupt: SSH

- Von außen ist die rzssh1 erreichbar
 - Host: `rzssh1.informatik.uni-hamburg.de`
 - Fingerprint:
`23:f8:1b:c4:d2:c0:0a:f0:15:11:76:64:62:07:cc:8c`
- Zugang unter Linux & Mac: `ssh rz-kennung@rzssh1.informatik.uni-hamburg.de`
- Zugang unter Windows: Putty
- Ein paar interessante Befehle:
 - `whoiswhere, who, w, quota -v, top, mc, getent passwd | grep 6keitzel`
 - Personensuche in toll: `/home/j2007/7fietkau/pub/person`

SSH Bedienung vereinfachen

Datei: `~/.ssh/config`

```
Host fbi
```

```
  Hostname rzssh1.informatik.uni-hamburg.de
```

```
  User 6keitzel
```

```
  ForwardX11 yes
```

```
  DynamicForward 7777
```

- Jetzt reicht: `ssh fbi`
- Zahlreiche weitere Optionen: `man ssh_config`

Automatisches einloggen via Public-Key Authentifizierung

Vorgehen unter Linux und Mac

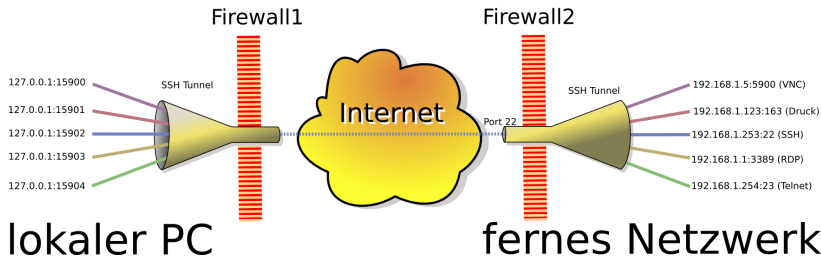
- Erstellen des Schlüsselpaars: `ssh-keygen`
- Ergebnis:
 - ~/.ssh/id_rsa (Private Key)
 - ~/.ssh/id_rsa.pub (Public Key)
- Übertragen des öffentlichen Schlüssels auf den Host:
`ssh-copy-id -i ~/.ssh/id_rsa.pub fbi`

Vorgehen unter Windows

- Erstellen des Schlüsselpaars mit `puttygen.exe`
- Manuelles Übertragen des öffentlichen Schlüssels auf den Host via `putty.exe`

Mithilfe von SSH TCP-Tunnel erstellen

Veranschaulichung SSH Tunneling



Dieses Bild basiert auf dem Bild 'SSHTunnel.png' aus der freien Mediendatenbank Wikimedia Commons und steht unter der GNU-Lizenz für freie Dokumentation. Der Urheber des Bildes ist Christian Mueller

Mithilfe von SSH TCP-Tunnel erstellen

Vorgehen unter Linux und Mac mit OpenSSH

- `ssh -L localPort:targetHost:targetHostPort viaServer`
Bsp: `ssh -L 3128:proxymh.uni-hamburg.de:3128 fbi`
- `ssh -D 7777 viaServer (SOCKS-Server)`
Bsp: `ssh -D 7777 fbi`

Vorgehen unter Windows mit Putty

- Analog zu Linux/Mac

Anwendungen transparent tunneln: tsocks

- 1 Konfigurationsdatei `/etc/tsocks.conf` anpassen:
 - 1 'Path' Auskommentieren
 - 2 `server = 127.0.0.1`
 - 3 `server_port = 7777`
 - 4 'local' eventuell anpassen
- 2 SOCKS-Server starten: `ssh fbi`
- 3 In neuer Shell tsocks starten
 - Alles was in dieser Shell gestartet wird geht durch den Tunnel
 - Alternative: `tsocks $anwendung`

Was ist mit grafischen Anwendungen?

Es gibt zwei Möglichkeiten

- X-Clients des RZ lokal anzeigen (falls X verfügbar):
`ssh -X host` oder in der `~/ssh/config`
- Den gesamten Bildschirminhalt via Screenshots übertragen:
 - 1 Zur einer starken Maschine verbinden (z.B. `rzdspc8`)
 - 2 Passwortdatei einrichten: `vncpasswd`
 - 3 VNC-Server inkl. X-Server starten: `vncserver`
 - 4 Auf dem eigenem Rechner einen VNC-Client starten, z.B.:
Linux: `vncviewer -via fbi rzdspc8:1`
Windows: Tunnel einrichten, dann über 'TightVNC'
 - Standard Fenstermanager: 'twm' - Andere möglich
 - Beenden des VNC-Servers mit: `vncserver -kill :1`

SCP mit FileZilla

- Für alle Plattformen erhältlich
- Hinweis: Benutzt sftp (ssh ftp)
- Alternative für Windows: WinSCP

SCP direkt aus der Shell

- Funktioniert wie `cp`, nur über Rechengrenzen hinweg
- `scp benutzerx@server1:datei1 datei2 benutzery@server2:`
 - `server1` oder `server2` kann auch lokal sein
- Bsp: `scp Dokument.pdf fbi:Desktop/` oder:
`scp -r fbi:SE1/Blatt02/ ~/data/studium/se1/`
- Achtung, Leerzeichen! Escapen oder in Hochkommata setzen

Transparente Einbindung ins Dateisystem

- Realisierung Über FUSE
- Einhängen:
`sshfs Benutzername@remoteHost:/path/ ~/sshfs`
Beispiel: `sshfs fbi: ~/fbi`
- Aushängen:
`fusermount -u ~/fbi`
- Dauerhafte Einbindung über fstab möglich

Drucken aus der Shell mit lpr

- lpr ist DAS Multifunktionsstool zum drucken
- Aufruf: `lpr -Pdrucker -o option dateiname`
- Vom Laptop: `cat doc.pdf | ssh fbi lpr -Pdrucker -o option dateiname`
- wichtige Drucker:
 - d105_hp: Für viele Ausdrücke
 - d105_hp8100: Für Din-A3 Drucke in schwarz-weiß
 - d116_hp**: Für kleine, schnelle Ausdrücke zum Selbstabholen
 - rz_fa4: Für DIN-A4 Farbdrucke
 - rz_fa3: Für DIN-A3 Farbdrucke
 - e120_hp**: Drucker im c.t

Drucken aus der Shell mit lpr

Auszug wichtiger Beispiele aus der Fachschafts-Wiki-Seite 'Drucken'

- 'Nicht' Doppelseitig drucken:
`lpr -Pdruckername -o sides=one-sided druckMich`
- Anzahl der Ausdrücke einstellen:
`lpr -Pdruckername -# anzahlDerAusdruecke druckMich`
- Nur spezielle Seiten drucken (Seiten 1-4 und 7, sowie 9-12):
`lpr -Pdruckername -o page-ranges=1-4,7,9-12
druckMich`
- Mehrere Seiten auf einem Blatt drucken: `lpr
-Pdruckername -o number-up=2 druckMich`
- Druckaufträge ansehen:
`lpq -a / lpq -Pdruckername`
- weitere Beispiele im Wiki

CUPS-Server lokal einbinden

- Drucker des RZ stehen lokal allen Anwendungen zur Verfügung
- Geht nur aus dem VPN heraus, da 'linuxprint:631' aufgelöst werden muss
 - Die Suchdomäne `informatik.uni-hamburg.de` muss explizit eingerichtet werden
- Unter Windows analog, nur über Samba

CUPS-Server lokal einbinden

Linux und Mac

- In `/etc/cups/cupsd.conf`:
 Browsing On
 BrowsePoll linuxprint
- CUPS neustarten: `/etc/init.d/cups restart`
- Im Druckdialog tauchen nun alle Drucker auf

Windows

- Drucker hinzufügen → 'Verbindung mit folgendem Drucker herstellen: `\\linuxprint\` eingeben → es erscheinen sämtliche Drucker
- Nur ein Drucker pro Durchgang kann eingerichtet werden

Danke für Eure Aufmerksamkeit