

Fernwartung des Schulservers übers Internet

Anleitung ssh - putty – winscp

- für Arktur v.3.5.2 bzw. v.3.5.6 -

Die folgende Anleitung beschreibt die Fernwartung des Schulservers z.B. von zu Hause über das Internet. Der Benutzer sollte sich im Klaren sein, dass er den zu wartenden Server durch die Öffnung nach außen potenziell gefährdet. Die Beschreibung orientiert sich daher auch an einer Datenübertragung mittels SSH.

Voraussetzung für die Fernwartung ist natürlich die Kenntnis der z.Zt. gültigen IP-Adresse. Die einfachste Lösung ist das Anlegen eines Accounts bei www.dyndns.org. Die Vorgehensweise hierfür wird im Anhang dieser Anleitung beschrieben.

1. Schlüssel generieren:

Die Erstellung eines privaten und öffentlichen Schlüssels ermöglicht, den SSH-Daemon so zu konfigurieren, dass ein Zugriff auf den Server nur dann von außen möglich wird, wenn auf der anderen Seite, also dem Client zu Hause, der entsprechende Part vorhanden ist:

- Als root anmelden und an der Konsole

```
ssh-keygen -t rsa1
```

eingeben. Im Ordner `/root/.ssh` befinden sich anschließend zwei Schlüssel: „identity“ und „identity.pub“.

Anmerkung: Falls man einem Kollegen ebenfalls Zugriff auf den Server von zu Hause aus geben möchte, etwa zum Hochladen von Arbeitsblättern, muss man dem Kollegen den Shellzugang erlauben (Sysadm-Menü: Anwender verwalten - einzelne Anwender verwalten - den Shell-Zugang eines Anwenders ändern - Lehrer - Name - Vollzugang mit Prompt; dann Aktivieren nicht vergessen). Nun unter dem Namen des Kollegen anmelden und den o.a. Befehl ausführen. Das Schlüsselpaar findet man dann im Verzeichnis des entsprechenden Users, genau unter `„/home/[Benutzername]/.ssh“`. Die weitere Vorgehensweise ist analog zu der für root.

- Schlüssel duplizieren: Den Schlüssel `identity.pub` nach `authorized_keys` kopieren:

```
cp /root/.ssh/identity.pub /root/.ssh/authorized_keys
```

- Schlüssel zum Client bringen: Den Schlüssel `identity` in das Verzeichnis des Clients kopieren, auf dem putty installiert ist. Am einfachsten geht das, indem man die Datei `identity` nach `/home/tmp` kopiert und erst einmal die Rechte ändert, so dass man sie anschließen von einem Client im Netz aus auf Diskette kopieren oder sich selbst per E-Mail schicken kann

```
cp /root/.ssh/identity /home/tmp  
chmod 666 /home/tmp/identity
```

- Man findet die Datei nun auf einem Client im Verzeichnis `t:`. Nach dem Kopieren dann auf jeden Fall löschen!

2. Den SSH-Zugang auf Arktur freigeben

In der Grundeinstellung ist der SSH-Zugang von außen durch die „Firewall-Regeln“ deaktiviert. Um den Zugang für eine Fernwartung zu ermöglichen, muss man als root in der Datei `/etc/sysconfig/ipfilter` editieren:

```
mcedit /etc/sysconfig/ipfilter
```

und in Zeile 18

```
WORLD_ACCESS="no"
```

ändern in

```
WORLD_ACCESS="yes"
```

Wenn man nur den SSH-Zugang erlauben möchte, was aus Sicherheitsgründen zu empfehlen ist, muss man die letzten Zeilen noch abändern in:

```
WORLD_ACCESS_SSH="yes"
```

```
WORLD_ACCESS_WWW="no"
```

```
WORLD_ACCESS_FTP="no"
```

Man speichert mit F2 und beendet mit F10.

Diese Änderungen werden übernommen mit:

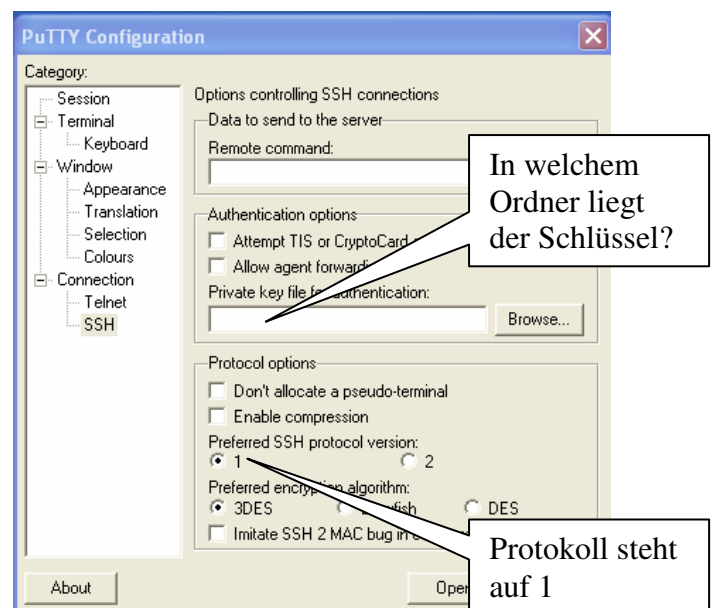
```
/etc/init.d/ipfilter reload
```

3. Auf dem entfernten Rechner: Schlüssel putty bekannt geben:

Im Putty-Konfigurations-Menü befindet sich unter connection der Menüpunkt SSH. Dort kann unter Private key file for authentication der Ordner angegeben werden, in dem jetzt die Datei identity abgelegt wurde. Unter SSH Protocol version muss als Version SSH 1 angegeben sein.

Das Einstellungsmenü neuerer Putty-Versionen sehen ggf. etwas anders aus; besonders der SSH-Abschnitt ist noch einmal in mehrere Fenster untergliedert. Die einzustellenden Optionen sind aber gleich:

1. Bei „Preferred SSH protocol version“ muss „1“ angewählt werden und
2. muss man den Pfad zum „Private key file“ mit der entsprechenden Datei („identity“) angeben. Diese Datei kann man bedenkenlos umbenennen.

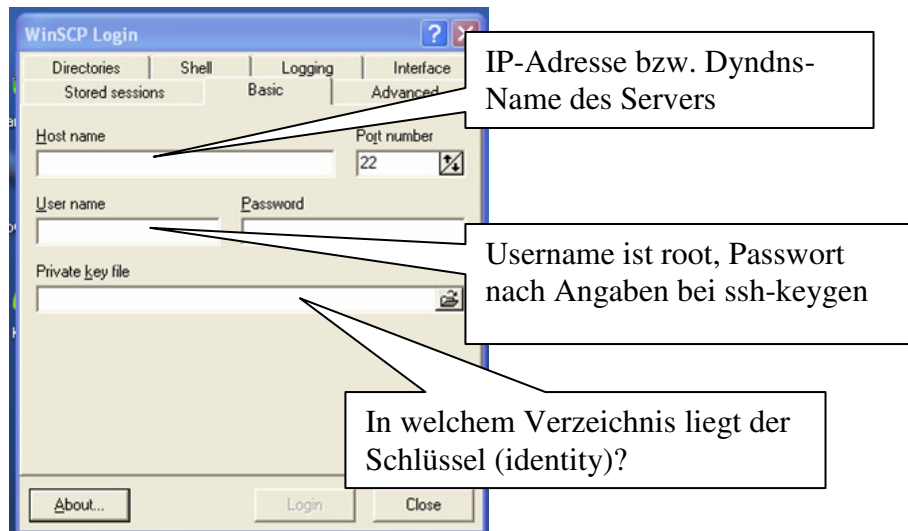


Die jeweils aktuelle Version von Putty findet man hier:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

4. Mit WINSCP Dateien kopieren

Mit WinSCP lässt sich von jedem Client-Rechner aus alles auf den Server oder vom Server zum heimischen PC kopieren. Das Programm kann wie putty mit den generierten Schlüsseln umgehen, ist selbsterklärend und dürfte relativ sicher sein. Eine funktionierende Version von WinSCP wird bei der Installation des Servers automatisch nach /home/adm/software/winscp kopiert, von Client aus zu finden unter p:\software\winscp.



Auch hier sehen die Konfigurationsfenster neuerer Versionen ggf. anders aus, inzwischen ist das Programm auch als „international“ zu laden, d.h. man kann als Sprache bei der Installation „deutsch“ als Sprache einstellen.

Die jeweils aktuelle Version von WinSCP findet man hier:

<http://winscp.sourceforge.net/eng/download.php>

Anhang

Einrichten eines Accounts bei www.dyndns.org (Vgl. Anleitung „Webserver“)

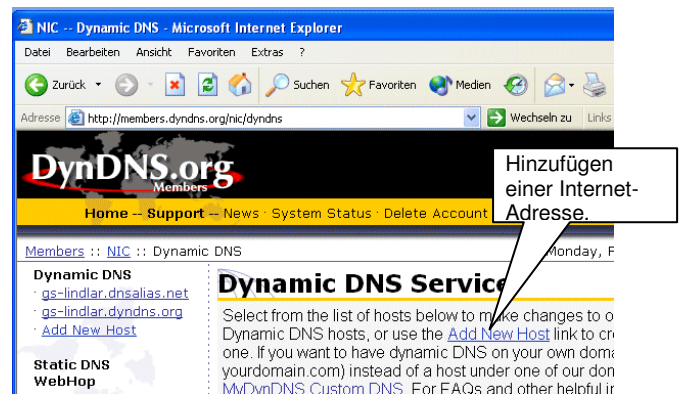
Einen professionellen Dienst bietet z.B. dyndns.org an. Bei der Eingabe einer dort beantragten Internetadresse wie z.B. <http://schulexyz.dyndns.org> sorgt dieses Service für die Weiterleitung an die richtige IP-Adresse. Damit wird der schulische Server auch hier weltweit immer unter derselben Adresse erreichbar.

Die IP-Adresse des schulischen Arkturs ändert sich mit jeder neuen Einwahl. Um also das oben beschriebene Verfahren durchführbar zu machen, muss diesem Dienstleister sofort nach der Einwahl von Arktur ins Internet automatisch die IP-Adresse übermittelt werden, die Arktur gerade zugeteilt bekommen hat. Das erledigt der Aufruf eines Scripts, das in die Datei `/etc/ppp/ip-up` eingebunden wird. Damit Arktur nicht offline geht, reicht ein regelmäßiges ping an irgendeine bekannte Webadresse aus.

Im Folgenden sei beispielhaft das Verfahren bei dyndns.org beschrieben. Zunächst sichert man sich eine entsprechende Internetadresse, z.B. schulexyz.dyndns.org. Dazu ruft man die Seite bei dyndns.org auf, lässt sich dort registrieren und erhält nach wenigen Minuten per Mail den Zugang zur Konfigurationsseite. Damit ist die Registrierung abgeschlossen.



Anschließend muss man nun die Internetadresse definieren, unter der der schulische Arktur erreichbar sein soll - auf der angesprochenen Webseite spricht man von einem Host bzw. man klickt auf **Add New Host**. In der folgenden Eingabemaske bestimmt man die Internetadresse, hier also z.B. schulexyz.dyndns.org.



Mit der Anmeldung hat man einen Benutzernamen und ein Passwort definieren können, mit denen man sich jederzeit wieder bei dyndns.org einloggen kann und die man benötigt, wenn man später mittels des bereits erwähnten Scripts Arktur seine IP-Adresse automatisch übermitteln lässt.

Auf Arktur 3.5.2 bzw. 3.5.6 findet man unter `/home/adm/software/linux` die Datei „`dyndns.zip`“. Wenn man diese Datei nach `/var/updates` kopiert und entpackt, kann man das Paket mit der Update-Funktion im `sysadm`-Menü einrichten.

Alternativ kopiert man es in das Wurzelverzeichnis (!) von Arktur, entpackt zunächst mit

```
unzip dyndns.zip
```

und entpackt nun das `tgz`-Archiv mittels

```
tar xzvf dyndnsupdate.tgz.
```

Beim Auspacken werden einige Dateien in verschiedene Unterverzeichnisse kopiert.

Die weiteren Schritte sind in der Version 3.5.2 bzw. 3.5.6 schon vorkonfiguriert. Man öffnet die Datei `/etc/ppp/ip-up-local`:

```
mcedit /etc/ppp/ip-up.local
```

und entfernt die Kommentarsymbole „#“ vor folgenden Zeilen und editiert entsprechend des eigenen Accounts bei dyndns „USERNAME“, „PASSWORD“ und „DYNHOSTNAME“

```
#USERNAME=foobar
#PASSWORD=eltodyndns
#IF=ppp0 # ppp0 bei TDSL, ipp0 bei ISDN
#LOG=/var/log/dyndnsupdate.log
#DYNHOSTNAME=foobar.homelinux.net
#/sbin/dyndnsupdate -d -i $IF -u $USERNAME:$PASSWORD -h $DYNHOSTNAME > $LOG
```

Wie immer speichern mit F2 und beenden mit F10.

Bei der nächsten Einwahl wird die aktuelle IP an dyndns geschickt und man ist - unabhängig von der jeweiligen IP - unter der eingetragenen Adresse erreichbar.

Um ggf. sicher zu stellen, dass Arktur nicht offline geht, muss noch der standardmäßig vorhandene Eintrag `/etc/ppp/inet-off` aus der crontab verändern oder entfernt werden. Zur Bearbeitung der crontab ruft man an der Konsole `crontab -e` auf.

Will man ein offline bzw. die Zwangstrennung von Arktur durch die Telekom grundsätzlich verhindern, fügt man in die crontab folgende Zeile ein:

```
0-59/5 * * * * ping -c1 -q www.irgendeineAdresse.de > /dev/null
```

Damit wird alle fünf Minuten eine ganz kurze Verbindung ins Internet hergestellt.

Jetzt ist Arktur per ssh immer über `http://schulexyz.dyndns.org` erreichbar.

Fragen und Rückmeldungen speziell zur Anpassung der Anleitung an die Arktur-Version v.3.5.2 bzw. v.3.5.6: mahr@medienzentrum-oberberg.de