Verschlüsseltes FTP

Da FTP ein unsicheres Protokoll ist, um Daten zu übertragen, gibt es hier ein HowTo, um den Login und den Datentransfer zu verschlüsseln

Installation

```
sudo apt-get install vsftpd openssl
```

SSL-Schlüssel erstellen

```
sudo openssl req -x509 -nodes -days 730 -newkey rsa:1024 -keyout
/etc/vsftpd.pem -out /etc/vsftpd.pem
chmod 600 /etc/vsftp.pem
```

Bei der Zertifikatserstellung werden folgende Fragen getstellt. Zur Identifikation ist es nötig, die richtigen Dinge einzutragen

```
Country Name (2 letter code) [GB]: Land (z.B. DE)
State or Province Name (full name) [Berkshire]: Bundesland (z.B. Bayern)
Locality Name (eg, city) [Newbury]: Stadt (z.B. München)
Organization Name (eg, company) [My Company Ltd]: eigener Name
Organizational Unit Name (eg, section) []: Bezeichnung des Dienstes (z.B.
FTP-Server)
Common Name (eg, your name or your server's hostname) []: Name, unter dem
der Rechner zu erreichen ist (z.B. www.microsoft.de)
Email Address []: eMail-Adresse
```

Datei mit Accounts erstellen, die sich nicht am FTP anmelden können

```
sudo -s
cat /etc/passwd | cut -d“:“ -f1 > /etc/vsftpd.user_deny
```

Aus der entstandenen Liste (es sind alle Benutzer enthalten) müssen die alle FTP-Nutzer herausgelöscht werden

Logfile für alle lesend setzen

```
sudo chmod go+r /var/log/vsftpd.log
```

Konfigurationsdateien

/etc/vsftpd.conf

vsftpd.conf

```
# daemon started from an initscript.
listen=YES
# Allow anonymous FTP? (Beware - allowed by default if you comment this
out).
anonymous_enable=NO
# Schalter, um Account aus einer Liste zugriff zu verbieten
userlist_enable=YES
# Liste mit zugriffsberechtigen usern
userlist_file=/etc/vsftpd.user_deny
# Uncomment this to allow local users to log in.
local_enable=YES
# Uncomment this to enable any form of FTP write command.
write_enable=YES
# Default umask for local users is 077. You may wish to change this to
022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
# Uncomment this to allow the anonymous FTP user to upload files. This
only
# has an effect if the above global write enable is activated. Also,
you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=NO
# Uncomment this if you want the anonymous FTP user to be able to
create
# new directories.
anon_mkdir_write_enable=NO
# Activate directory messages - messages given to remote users when
they
# go into a certain directory.
dirmessage_enable=YES
# Activate logging of uploads/downloads.
xferlog_enable=YES
# Make sure PORT transfer connections originate from port 20 (ftp-
data).
connect_from_port_20=YES
# You may override where the log file goes if you like. The default is
shown
# below.
xferlog_file=/var/log/vsftpd.log
# If you want, you can have your log file in standard ftpd xferlog
format
xferlog_std_format=YES
# You may change the default value for timing out an idle session.
```

```
idle_session_timeout=600
# You may change the default value for timing out a data connection.
data_connection_timeout=120
# You may fully customise the login banner string:
ftpd_banner="Welcome to da-checka's FTP."
chroot_local_user=YES
# This option should be the name of a directory which is empty.  Also,
the
# directory should not be writable by the ftp user. This directory is
used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
# Einstellungen fuer ssl-verschluesselung
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=NO
force_local_logins_ssl=NO

ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO

# This option specifies the location of the RSA certificate to use for
SSL
# encrypted connections.
rsa_cert_file=/etc/vsftpd.pem

# Diese Option gibt an, dass die Lokale Systemzeit und nicht GMT
genutzt wird
use_localtime=YES

# Einstellungen fuer den SSL-verschluesselten Datenverkehr von aussen
# Die angegebenen Ports muessen in der FritzBox weitergeleitet werden
#pasv_addr_resolve=yes
#pasv_address=da-checka.ath.cx
pasv_min_port=22000
pasv_max_port=22015
pasv_promiscuous=YES
setproctitle_enable=YES
session_support=YES
```

Sicherheitseinstellung

Da Filezilla ab Version 3.5.3 die Cipher-Suite verändert hat, muss man die Konfiguration von vsftpd

anpassen. Hierzu einfach folgende Zeile an die Konfigurtion anhängen

vsftpd.conf

```
ssl_ciphers=HIGH
```

Skripte für FTP

Das Leben ist zu kurz zum tippen, deshalb hier ein paar Scripte, um mir ein paar Arbeiten zu erleichtern

- Skript zur erstellung eines FTP-Benutzers findet man hier.
- Script zum löschen eines FTP-Benutzers findet man hier.
- ftpwho für vsftpd findet man hier.

Bug bei bei chroot

In der Version 2.3.5, die bei ubuntu und Debian standardmäßig ausgeliefert wird, gibt es einen Bug #656900.

Dieser ist bekannt und wurde in der Version 3 behoben. Leider wird Version 3 nicht bei Debian und Ubuntu ausgeliefert.

Zum fixen den Bugs eignet sich folgende Methoden

```
echo "deb http://ftp.cyconet.org/debian wheezy-updates main non-free
contrib" >> /etc/apt/sources.list.d/wheezy-updates.cyconet.list
aptitude update
aptitude install -t wheezy-updates debian-cyconet-archive-keyring vsftpd
echo "allow_writeable_chroot=YES" >> /etc/vsftpd.conf
/etc/init.d/vsftpd restart
```

Und alles läuft wieder wie gewünscht

Quellen

- http://wiki.ubuntuusers.de/vsftpd
- http://ibohm.blogspot.de/2012/02/gnutls-error-12-tls-fatal-alert-has.html
- http://www.redirect301.de/filezilla-gnutls-error-12.html
- http://blog.waja.info/2013/05/13/500-oops-vsftpd-refusing-to-run-with-writable-root-inside-chroot/