

Linux (allgemein): proFTPD mit TLS

Was ist TLS, FTPS und SFTP?

TLS ([Transport Layer Security](#)) beschreibt einen weiteren Layer im Netzwerk-Protokoll. Hier wird im Gegensatz zum normalen TCP/IP das Datenpaket verschlüsselt übersendet. Da es aber nicht zu den standard Layern gehört wird es künstlich drüber gestülpt. D.h. jede Software die dies Nutzen will muß das TLS-Protokoll eigenständig implementieren.

Im Falle von proFTPs ist es das FTPS-Protokoll. ([FTP over SSL](#)) wie sie in der [RFC 4217](#) beschrieben wird.

SFTP ([SSH File Transfer Protocol](#)) hingegen basiert auf dem SSH-Protokoll und ist vergleichbar mit einer FTP-Verbindung, die per SSH getunnelt wird.

TLS für proFTPD

Dafür wird der `mod_tls` benötigt. I.d.R. ist er bei modernen Installationen von proFTPD schon vorhanden und muß lediglich aktiviert werden. Wenn nicht, muß man updaten oder proFTPD aus den Quellen selber kompilieren.

Die Datei `/etc/proftpd.conf` muß entsprechend ergänzt werden:

```
# TLS
<IfModule mod_tls.c>
  TLSEngine on
  TLSLog /var/log/proftpd/proftpd_tls.log
  TLSProtocol TLSv1
  TLSRequired off
  TLSVerifyClient off
  TLSRSACertificateFile /etc/ssl/certs/proftpd.cert.pem
  TLSRSACertificateKeyFile /etc/ssl/certs/proftpd.key.pem
</IfModule>
```

Hier werden als Beispiele das Zertifikat und der Key in den std. Debian-Verzeichnis für Zertifikate geholt. Auf anderen Systemen kann das natürlich auch woanders sein. Auch das TLS-Protocol kann variieren. Z.B. gibt es auch [SSLv23](#) und [SSLv3](#).

Achtung: Natürlich muß danach der proFTPD die Konfiguration neu einlesen:

```
/etc/init.d/proftpd restart
```

Eigene Zertifikate erstellen

Dafür brauchen wir das openssl-Paket (installieren, falls noch nicht vorhanden):

```
openssl req -new -x509 -days 365 -nodes \
-out /etc/ssl/certs/proftpd.cert.pem \
```

Linux (allgemein): proFTPD mit TLS

```
-keyout /etc/ssl/certs/proftpd.key.pem
```

Eindeutige ID: #1178

huschi

2006-06-26 14:09