

## Pure-FTPd mit TLS-Support

Peer Hartleben  
eMail: linux@peer2peer.it  
vom 19.01.2005  
Betriebssystem: ab SuSE 9.0

Der pure-FTP-Dämon unterstützt seit Version 1.0.16 die verschlüsselte Übertragung der Authentifizierungsdaten (Benutzername/Passwort). Auf einem aktuellen SuSE-Linux ist er relativ schnell eingerichtet.

### Folgende Tools sollten bereits installiert sein:

- make
- gcc/gcc++
- openssl
- pure-ftpd + sources
- Zertifikat in /etc/ssl/private/pure-ftpd.pem

Das Standardpaket wird ohne TLS-Support installiert. Um die Verschlüsselung nachträglich einzubinden, benötigen wir die Programmquellen, denn pure-FTPd muss neu übersetzt werden - diesmal mit TLS-Support. Im ausgepackten Quellverzeichnis rufen wir folgende Kommandos auf:

```
$> ./configure --with-tls
```

...übersetzt den Quellcode mit TLS-Support. Wer möchte, kann an dieser Stelle gleich noch weitere Parameter mitgeben. Mögliche Parameter sind:

```
--with-ldap=/usr/share/openldap
```

LDAP-Unterstützung wird einkompiliert. Der Pfad muss gegebenenfalls an die eigene Installation angepasst werden

```
--with-cookie
```

Es kann beim Verbinden auf den Server ein Begrüßungstext ausgegeben werden

```
--with-language=english
```

Es werden englischsprachige Messages ausgegeben

```
--with-paranoidmsg
```

Standard-Fehlermeldungen anstelle spezifischer bei Loginversuchen

```
--with-tls
```

SSL/TLS Support, damit wir ftps verwenden können

```
--with-quotas
```

Virtuelle Userquotas können verwendet werden - Systemquotas sind dazu nicht nötig

```
--with-virtualchroot
```

normale User können ihr eigenes Homedirectory nicht verlassen, es ist jedoch möglich, symbolische Links auf andere Verzeichnisse anzulegen.

```
--with-privsep
```

Privilege Separation. Das heisst, dass nur der Hauptprozess unter root läuft

```
--without-humor
```

Ohne 'Funny Messages'

```
--without-banner
```

Es wird nach dem Login kein Banner angezeigt

Wurde alles korrekt ausgeführt, können wir die Installation beginnen:

```
$> make install-strip
```

Jetzt muss dem pure-FTPD nur noch gesagt werden, dass er TLS verwenden soll. Entweder der Daemon wird mit der entsprechenden Option aufgerufen:

```
/usr/local/sbin/pure-ftpd --tls=1 &
```

oder Sie schreiben es in seine Konfigurationsdatei /etc/pure-ftpd.conf:

```
TLS 1
```

Die Bedeutung der einzelnen Schalter:

TLS 1 Es können Clients mit oder ohne SSL/TLS Layer connecten.

TLS 2 Es ist ausschließlich SSL/TLS möglich. Andere Verbindungen werden nicht akzeptiert.

TLS 0 TLS ist deaktiviert.

Anschließend kann der FTP-Server ganz normal gestartet werden. Mit einem FTP-Client können wir die neue Funktion testen. Am besten eignet sich dafür lftp, da er auch TLS unterstützt:

```
$> lftp localhost -u testuser -d
```

```
  Password:
```

```
    lftp testuser@localhost:~> dir
    ---- Connecting to localhost (127.0.0.1) port 21
    <--- 220-FTP server ready.
    <--- 220-<<
    <--- 220-**
    <--- 220-** Welcome to the Manpage Example FTP-Server
    <--- 220-**
    <--- 220-**
    <--- 220-** Anonymous Login is allowed, please send your
    <--- 220-** REAL e-Mail Address as Password. Thankyou!
    <--- 220-**
    <--- 220 >>
    ---> FEAT
    <--- 211-Extensions supported:
    ...
    ---> AUTH TLS
    <--- 234 AUTH TLS OK.
    ...
    WARNING: Certificate verification: self signed certificate
    ....
```

So oder ähnlich sollte das Ergebnis aussehen.

Weiterführende Quellen:

<http://www.manpage.ch/faq/ftpdirectories.php>