9.3 FTP-Server mit Pure-FTPd

Jail-Name	IP-Adresse	Funktion
www	10.0.0.2	Web- und FTP-Server

Die wohl bekannteste Methode, um Daten auf einen Server zu übertragen, ist die Nutzung des »File Transfer Protocol«, kurz FTP.

Hinweis: Falls nur eine überschaubare Zahl von Benutzern Dateien auf den Server übertragen können soll, ist in vielen Fällen die Nutzung von SCP/SFTP – einem Datei-Transfer-Protokoll über SSH – ausreichend. Verbinde Dich dazu einfach per SCP-Client über den SSH-Port Deines Servers, und nutze die Zugangsdaten Deines Systembenutzers zur Anmeldung. Beim Anlegen weiterer Benutzer musst Du eine gültige Shell angeben, also beispielsweise /bin/sh.

Wir nutzen für die Übertragung von Dateien auf den Server Pure-FTPd. Dieser FTP-Server ist sicher, sehr performant und sehr flexibel. In diesem Buch installieren wir ihn in unserer Webserver-Jail mithilfe des Ports `ftp/pure-ftpd`. Bei den Kompilieroptionen wählen wir die folgenden aus:

- [MYSQL]
- [PRIVSEP]
- [PERUSERLIMITS]
- [THROTTLING]
- [UTF8]
- [SENDFILE]
- [LARGEFILE]

Hinweis: Du kannst natürlich Pure-FTPd auch in einer eigenen Jail betreiben.

Wir wählen `[MYSQL]` aus, weil wir die Benutzerverwaltung über MySQL vornehmen werden. So können wir über ein Datenbank-Verwaltungstool – beispielsweise PHPMyAdmin – sehr komfortabel Benutzer anlegen, bearbeiten und löschen.

Hinweis: Pure-FTPd bringt auch eine eigene MySQL-unabhängige Benutzerverwaltung mit. Details zur Benutzung findest Du in den Man-Pages zu `pure-pw`.

Nach der Installation legen wir den Systembenutzer `ftp` an, unter dem wir Pure-FTPd betreiben werden.

```
# pw user add ftp -u 21 -s /sbin/nologin
```

Als Konfigurationsparameter setzen wir die folgenden Werte in der Datei `/usr/local/etc/pure-ftpd.conf`. Auch hier sind die fett gedruckten Parameter an Deine eigenen Anforderungen anzupassen. `xxx.xxx.xxx.xxx` steht hierbei für die externe IP-Adresse Deines Servers, über die der FTP-Server erreichbar sein soll.

```
ChrootEveryone   yes
BrokenClientsCompatibility   yes
MaxClientsNumber   50
Daemonize   yes
MaxClientsPerIP   4
VerboseLog   no
DisplayDotFiles   yes
AnonymousOnly   no
NoAnonymous   yes
AnonymousCanCreateDirs   no
SyslogFacility   ftp
DontResolve   yes
MaxIdleTime   15
LimitRecursion   10000   8
MaxLoad   4
PassivePortRange   30000   50000
ForcePassiveIP   xxx.xxx.xxx.xxx
AntiWarez   yes
Bind   10.0.0.2,21
Umask   137:027
MinUID   1000
AllowUserFXP   yes
AllowAnonymousFXP   no
ProhibitDotFilesWrite   no
ProhibitDotFilesRead   no
AutoRename   no
AnonymousCantUpload   yes
CreateHomeDir   yes
MaxDiskUsage   99
CustomerProof   yes
MySQLConfigFile   /usr/local/etc/pureftpd-mysql.conf
```

`ChrootEveryone` legt fest, ob alle Benutzer in ihrem Homeverzeichnis eingesperrt werden sollen. Diese Einstellung ist empfohlen, da es den FTP-Benutzern sonst gegebenenfalls möglich ist, Deinen gesamten Server bzw. die gesamte Jail zu durchsuchen.

Mit `MaxClientsNumber` kannst Du die Obergrenze der gleichzeitigen Client-Verbindungen zum Server definieren. Sind in unserem Fall 50 FTP-Clients mit dem Server verbunden, werden weitere Verbindungsversuche abgewiesen.

Der Parameter `MaxClientsPerIP` legt fest, wie viele gleichzeitige Client-Verbindungen von einer IP-Adresse ausgehen können.

Falls Du Probleme mit Pure-FTPd hast, kannst Du durch Setzen des Parameters `VerboseLog` auf `yes` etwas ausführlichere Log-Einträge erstellen lassen.

Mit den Parametern `AnonymousOnly`, `NoAnonymous` und `AnonymousCanCreateDirs` steuern wir die Zugriffsberechtigungen von nicht autorisierten, also anonymen Benutzern.

Der Parameter `PassivePortRange` legt den bisher ungenutzten Port-Bereich fest, den Pure-FTPd für die Client-Verbindungen nutzen darf. Diesen müssen wir später auch in der Firewall freigeben (siehe Kapitel 9.3.2, »Firewall anpassen«).

Mit `ForcePassiveIP` geben wir die IP-Adresse an, die Pure-FTPd als eigene IP-Adresse verwenden soll.

Der Parameter `Bind` legt fest, dass sich Pure-FTPd an die interne IP-Adresse der Jail binden und auf Port `21` lauschen soll. Der Port `21` ist der Standard-FTP-Port.

Wenn neue Dateien oder Verzeichnisse auf den Server geladen werden, müssen diese eine Berechtigung erhalten. Der Benutzer und die Gruppe sind durch den Benutzer festgelegt, der die Daten hochlädt. Die standardmäßige Lese- und Schreibberechtigung wird durch den Parameter `Umask` definiert. Die Rechte vor dem Doppelpunkt spiegeln die Dateirechte wider, die Rechte dahinter sind die Verzeichnisrechte.

Hinweis: Die Umask enthält die Rechte, die einer Datei oder einem Verzeichnis entzogen werden sollen – ausgehend von der höchsten Berechtigung 777 (Lesen, Schreiben und Ausführen für den Besitzer, die Gruppe und alle anderen). Die hier angegebene Umask erzeugt demnach Dateien mit der Berechtigung 640 (777 - 137) und Verzeichnisse mit 750 (777 - 027).

Die Benutzerdaten beziehen wir aus einer MySQL-Datenbank. Die Verbindungsdaten zum MySQL-Server sind in der Datei `/usr/local/etc/pureftpd-mysql.conf` abgelegt. Ihren Speicherort haben wir im Parameter `MySQLConfigFile` angegeben. Darin definieren wir auch die Datenbankabfragen, über die Pure-FTPd seine Zugangsdaten bezieht.

Hinweis: Auch für Pure-FTPd empfehle ich einen eigenen MySQL-Benutzer mit eigener Datenbank und lediglich SELECT-Berechtigung anzulegen. Die Zugangsdaten sind entsprechend hier zu pflegen.

```
MYSQLServer   10.0.0.1
MYSQLPort     3306
MYSQLUser     db_pureftpd
MYSQLPassword <DAS-DB-PUREFTPD-PASSWORT>
MYSQLDatabase db_pureftpd
MYSQLCrypt    md5

# \L is replaced by the login of the user trying to authenticate.
# \I is replaced by the IP address the user connected to.
# \P is replaced by the port number the user connected to.
# \R is replaced by the IP address the user connected from.
# \D is replaced by the remote IP address, as a long decimal number.

MYSQLGetPW    SELECT password FROM users WHERE user="\L" AND \
   status="1" AND (ipaccess="*" OR ipaccess LIKE "%\R%")
MYSQLGetUID   SELECT uid FROM users WHERE user="\L" AND \
   status="1" AND (ipaccess="*" OR ipaccess LIKE "%\R%")
MYSQLGetGID   SELECT gid FROM users WHERE user="\L" AND \
   status="1" AND (ipaccess="*" OR ipaccess LIKE "%\R%")
MYSQLGetDir   SELECT dir FROM users WHERE user="\L" AND \
   status="1" AND (ipaccess="*" OR ipaccess LIKE "%\R%")
MySQLGetQTAFS   SELECT quotafiles FROM users WHERE \
   user="\L" AND status="1" AND (ipaccess="*" OR ipaccess LIKE "%\R%")
MySQLGetQTASZ   SELECT quotasize FROM users WHERE \
   user="\L" AND status="1" AND (ipaccess="*" OR ipaccess LIKE "%\R%")
MySQLGetBandwidthUL   SELECT ulbandwidth FROM users \
   WHERE user="\L" AND status="1" AND (ipaccess="*" OR \
   ipaccess LIKE "%\R%")
MySQLGetBandwidthDL   SELECT dlbandwidth FROM users WHERE \
   user="\L" AND status="1" AND (ipaccess="*" OR ipaccess LIKE "%\R%")
```

Um Pure-FTPd beim Start der Jail ebenfalls mit zu starten, müssen wir folgende Zeile in die `/etc/rc.conf` eintragen:

```
pureftpd_enable="YES"
```

Anschließend können wir Pure-FTPd bereits starten. Daten übertragen können wir aber noch nicht, da wir zunächst noch Benutzer anlegen müssen.

Pure-FTPd: http://www.pureftpd.org/

9.3.1 FTP-Benutzer anlegen

Die Benutzerverwaltung erfolgt in unserem Szenario über die in der Konfiguration angegebene Tabelle `users` in der Datenbank `db_pureftpd`. Das Passwort wird dabei als MD5-Hash hinterlegt. Benutzerspezifische Einstellungen können hier ebenfalls gesetzt werden. Zunächst müssen wir allerdings die Tabelle `users` anlegen.

```
CREATE TABLE `db_pureftpd`.`users` (
   `user` varchar( 16  )   NOT NULL DEFAULT '',
   `status` enum( '0', '1' )   NOT NULL DEFAULT '0',
   `password` varchar( 64 )   NOT NULL DEFAULT  '',
   `uid` varchar( 11 )   NOT NULL DEFAULT  '-1',
   `gid` varchar( 11 )   NOT NULL DEFAULT  '-1',
   `dir` varchar( 128 )   NOT NULL DEFAULT  '',
   `ulbandwidth` smallint( 5 )   NOT NULL DEFAULT  '0',
   `dlbandwidth` smallint( 5 )   NOT  NULL DEFAULT '0',
   `comment` tinytext   NOT NULL,
   `ipaccess` varchar( 255 )   NOT NULL DEFAULT '*',
   `quotasize` smallint( 5 )   NOT NULL DEFAULT '0',
   `quotafiles` int( 11 )   NOT NULL DEFAULT '0',
      PRIMARY  KEY ( `user` ) )
   ENGINE = InnoDB
   DEFAULT CHARSET = utf8;
```

Einen Benutzer kannst Du mit jedem MySQL-Client Deiner Wahl anlegen. Die Spalten haben folgende Bedeutung:

- `user`: Benutzername
- `status`: 1 = aktiv, 0 = gesperrt
- `password`: Passwort als MD5-Hash
- `uid`: Benutzer-ID (siehe /etc/passwd)
- `gid`: Gruppen-ID (siehe /etc/group, beispielsweise 80 für www)
- `dir`: Homeverzeichnis des Benutzers
- `ulbandwidth`: Maximale Upload-Bandbreite in kb/s
- `dlbandwidth`: Maximale Download-Bandbreite
- `comment`: Kommentar zum Benutzer
- `ipaccess`: Anmeldung nur von diesen IP-Adressen erlauben, * (Sternchen), wenn von allen der Zugriff gestattet ist
- `quotasize`: Maximal belegbarer Speicherplatz in MB
- `quotafiles`: Maximale Anzahl an Dateien

Den MD5-Hash des Passworts kannst Du mithilfe des folgenden Befehls erstellen:

```
# md5 -qs <PASSWORT>
```

9.3.2 Firewall anpassen

Wir müssen in der Firewall den Port-Range 30000 bis 50000 sowie den Port 21 für eingehende Verbindungen freigeben, da wir diese für den passiven Modus in der `pure-ftpd.conf` angegeben haben (Parameter: `PassivePortRange`) bzw. weil Pure-FTPd standardmäßig auf Port 21 lauscht.

Hinweis: Auch hier kannst Du die gefühlte Sicherheit erhöhen, indem Du Pure-FTPd auf einem anderen Port als 21 lauschen lässt. Dies kannst Du aber auch über die Firewallregeln steuern.

```
rdr on $if proto tcp from any to $if port { 21, 30000:50000 } -> $www
```

Diese Regel leitet Anfragen auf dem Interface `$if`, die auf den Ports `21` bzw. `30000` bis `50000` ankommen, an die Webserver-Jail weiter.

9.4 Mailserver mit IMAP und POP3

Jail-Name	IP-Adresse	Funktion
mail	10.0.0.3	Mailserver

Einen Mailserver zu konfigurieren ist für einen Einsteiger eines der schwersten Unterfangen überhaupt. Nicht nur, weil sich ein funktionierender Mailserver aus mehreren Diensten zusammensetzt, sondern auch, weil er noch immer zu den Top-Zielen von Cyber-Angriffen zählt.

Beim letzten Punkt geht es nicht nur darum, dass ungesicherte Mailserver für den Versand von Spam und Schadsoftware missbraucht werden, sondern auch um die Übermittlung solcher Software bis auf das System eines Benutzers.

Wir werden uns also einen Mailserver konfigurieren, der nur den registrierten Benutzern und den Systemprozessen den Versand von Nachrichten erlaubt, Schadsoftware wie Viren und Trojaner bereits auf dem Server bestmöglich herausfiltert und die Übermittlung von Spam verhindert.

Gleichzeitig werden wir das ein oder andere Plug-in konfigurieren, um die Qualität der Filterung stetig zu verbessern, ohne dass die Benutzerfreundlichkeit darunter leidet.

Hinweis: Die Anmeldedaten, wie Benutzername und Passwort, werden wir in einer Datenbank auf unserem MySQL-Server speichern. Es ist daher Voraussetzung, dass der Datenbankserver bereits installiert und konfiguriert ist.

Wir werden Dovecot für die Nutzung des POP3- und IMAP-Protokolls konfigurieren. Vereinfacht gesagt, ist bei der Nutzung von POP3 der Client für die dauerhafte Speicherung der E-Mails verantwortlich, da nach dem Abrufen in der Regel die Nachrichten vom Server gelöscht werden. Bei der Nutzung von IMAP verbleiben die E-Mails dagegen dauerhaft auf dem Server, sodass sie von überall zugänglich sind. Es gibt demnach nur einen zentralen Speicherort, was die Nutzung von verschiedenen Clients aus vereinfacht (Gruppenpostfächer).